DEPARTMENT OF HOMELAND SECURITY

DATA PRIVACY AND INTEGRITY ADVISORY COMMITTEE

(DPIAC)

1:00 p.m.

Friday,

May 14, 2021

(VIA MICROSOFT TEAMS)
APPEARANCES

COMMITTEE MEMBERS:

Sharon Anolik
Dennis Dayman (DPIAC Policy Subcommittee Chair)
Mark Francis
Lynn Goldstein
Sarah Knight
John Kropf
Chris Pahl
Tom Plofchan
Lisa Sotto (Chairperson)
Chris Teitzel (Emerging Technologies Subcommittee Chairperson)
Surbhi Tugnawat
Ron Whitworth

ALSO PRESENT:

Nicole Sanchez, Designated Federal Official
<table>
<thead>
<tr>
<th>Page</th>
<th>AGENDA</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Call to Order and Roll Call</td>
</tr>
<tr>
<td>6</td>
<td>Nicole Sanchez, Designated Federal Official</td>
</tr>
<tr>
<td>7</td>
<td>Privacy Office U.S. Department of Homeland Security</td>
</tr>
<tr>
<td>7</td>
<td>Chairperson Remarks</td>
</tr>
<tr>
<td>9</td>
<td>Lisa Sotto, Chairperson Data Privacy and Integrity Advisory Committee</td>
</tr>
<tr>
<td>9</td>
<td>Chief Privacy Officer Remarks</td>
</tr>
<tr>
<td>11</td>
<td>Lynn Parker Dupree, Chief Privacy Officer</td>
</tr>
<tr>
<td>12</td>
<td>U.S. Department of Homeland Security</td>
</tr>
<tr>
<td>14</td>
<td>Tasking Update - DPIAC Policy Subcommittee</td>
</tr>
<tr>
<td>14</td>
<td>Dennis Dayman, DPIAC Policy Subcommittee Chair</td>
</tr>
<tr>
<td>29</td>
<td>Tasking Update - DPIAC Emerging Technologies Subcommittee</td>
</tr>
<tr>
<td>40</td>
<td>Chris Teitzel, Emerging Technologies Subcommittee Chair</td>
</tr>
<tr>
<td>41</td>
<td>Public Comments</td>
</tr>
<tr>
<td>41</td>
<td>Closing Statements and Meeting Adjournment</td>
</tr>
</tbody>
</table>

1
* MS. SANCHEZ: Good afternoon and welcome everyone. It is now just past one o'clock and this meeting of the Data Privacy and Integrity Advisory Committee is called to order.

We have committee members and members of the public with us today. Please everyone remember to mute your mics, until it is time for Q&A or time for public comments. And committee members, if you have any difficulties hearing or seeing at any time, just let me know.

The meeting agenda for today's session can be found on the Data Privacy and Integrity Advisory Committee website at dhs.gov/privacy-advisory-committee and from there you can look under meeting information and find today's date. The meeting information for today's meeting will also be found at that location later.

Let’s see. I will now take a quick roll call and turn it over to the Committee Chairperson Lisa Sotto for opening remarks.
1 Do we have Sharon Anolik?

2 MS. ANOLIK: Here.

3 MS. SANCHEZ: I see you Sharon. Thank you,

4 Dennis Dayman.

5 MR. DAYMAN: I’m here. Thank you.

6 MS. SANCHEZ: If you guys can go off mute. I
can't see all of you on my screen at once.

7 MR. DAYMAN: Nicole, Dennis is here. Can you
hear me? Hello?

8 MS. SANCHEZ: Okay, Dennis I see you. I'm
going to come back to you and do a comms check.

9 Mark Francis?

10 MR. FRANCIS: Hi, I'm here.

11 CHAIRPERSON SOTTO: Nicole, I think you're
having trouble hearing because I'm hearing both
Dennis and Mark.

12 MS. SANCHEZ: Okay, I can hear you, Lisa. So
that's good.

13 CHAIRPERSON SOTTO: Okay, Dennis and Mark
said yes.

14 MS. SANCHEZ: Wonderful, thank you. Sarah
Knight?
MS. KNIGHT: Yes, I'm here.

MS. SANCHEZ: Thank you. John Kropf?

MR. KROPF: Yes, I'm here.

MS. SANCHEZ: All right. Chris Pahl?

MR. PAHL: Yes, I'm here.

MS. SANCHEZ: Charles Palmer? Tom Plofchan?

MR. PLOFCHAN: Good afternoon.

MS. SANCHEZ: Hi, Lisa Sotto. I see you, thank you.

Chris Teitzel?

MR. TEITZEL: Here.

MS. SANCHEZ: Great. Surbhi Tugnawat.

MS. TUGNAWAT: Here.

MS. SANCHEZ: Thank you. Toke Vandervoort, I do not believe will be joining us today, but just in case. And Ron Whitworth?

MR. WHITWORTH: Yes, I'm here. Hello.

MS. SANCHEZ: Thank you Ron. All right, thank you all again for joining us today and now I will turn it over to -- yes?

CHAIRPERSON SOTTO: Lynn Goldstein, I believe.
MS. GOLDSTEIN: Yes, I'm here.

MS. SANCHEZ: Oh, I'm sorry, I jumped right
over Lynn, thank you Lisa.

MS. GOLDSTEIN: Thank you, Lisa.

MS. SANCHEZ: All right, over to you, Lisa.

Thank you.

* CHAIRPERSON SOTTO: Fantastic, thank you and
thank you all for joining. You know, it is less
than an ideal setting but I think, you know, we're
making do, I think, very well.

So Nicole, thank you for introducing everyone
today and thank you all, committee members and
members of the public for joining us and welcome to
this meeting of the Data Privacy and Integrity
Advisory Committee.

Before we begin, I would like to just remind
everyone to please mute your mics for the duration
of the presentations. There is designated time for
committee member questions after each presentation
and we’ll make sure that everybody gets time to ask
questions.

There's also designated time for public
comment at the end of the session.
For any members of the public who would like
to address the committee, please email
“PrivacyCommittee@hq.dhs.gov” and we'll do that
during the public comment portion of the session.
So, as I said, welcome to committee members,
to speakers, and to members of the public. And
we're going to, please ask that you use the chat
function if you wish to speak. It's, we usually
turn our tent cards up when we're meeting live but
we don't have that benefit over video conference.
So we have a great agenda today. We have our
new Chief Privacy Officer and Chief Freedom of
Information Act Officer, Lynn Parker Dupree, who is
joining us and is going to provide the committee
with an update on the Privacy Office’s activities.
Following Ms. Dupree’s presentation we're
going to receive updates from the Policy Committee
and the Emerging Technologies Subcommittee on their
progress with respect to their respective taskings.
And as I said, there'll be time after those
presentations for committee member Q&A after each
subcommittee briefing.

And as a reminder, the tasking information is available on the DPIAC webpage under meeting information for October 27, 2020.

Following these discussions, we've reserved time for public comments beginning tentatively at 2:40 and again, tentatively. We haven't received any advance notice from anyone who would like to address the committee. So we'll open the floor to members of the public around that time but if we are running ahead on discussion we may open the public comment period sooner. So I just want to stress that that may happen.

So again, please mute your mics, I will do the same, unless you're presenting or speaking during Q&A and I'd like to turn the program over to Chief Privacy Officer Lynn Barker Dupree.

* MS. PARKER DUPREE: Thank you so much. Good afternoon everyone and thank you for joining us for today's public meeting of the DPIAC. I'm very happy to have the opportunity to speak to the committee, and to hear updates on your work on
behalf of the public.

The DPIAC is the Privacy Office’s only advisory committee, and you all provide valuable insight and input to our important mission. I look forward to engaging with all of you this year. I've been enjoying my introductory meetings, and I'll be in taking into account all of your wonderful insights as we plan it for the year ahead.

Now while this is my first public meeting with the DPIAC as the Chief Privacy Officer, as I said before, in many ways, this is a homecoming for me. My first job in Privacy was in the DHS Privacy Office, and it is truly a full circle moment for me to be back in this capacity.

After serving in the Privacy Office, I transitioned to the Office of the General Counsel before going to the White House as a Deputy Associate Counsel for Presidential Personnel. I joined the Privacy and Civil Liberties Oversight Board and held a variety of roles there prior to my departure in 2020 as the Executive
Director. After leaving the PCLOB, I worked in the private sector as the Director of Governance and Controls in the Data Ethics and Privacy Office at Capital One.

I'm excited to be rejoining the Department at this critical time. The Department's programs and activities have continued to expand since its creation, and the technology has continued to evolve in ways that have had an outsized impact on personal privacy.

My priority is to ensure that the DHS Privacy Office is equipped to adapt and to respond to the changing realities in privacy issues. Part of accomplishing this goal means ensuring that we have a seat at the table in the discussions, early in the process whenever policies and programs that impact privacy are under development, and that we are fully utilizing our compliance processes to ensure that protections are embedded into programs and systems.

I'm also dedicated to ensuring that we are supporting our privacy colleagues in the
components, and that we are giving them the support and tools they need to ensure that the Department simultaneously protects privacy while meeting it's very important mission set.

As committee members, I appreciate the time commitment you have made and want to make the most out of your expertise to provide tangible and achievable recommendations to the Department. Going forward, you can expect to meet at least twice a year. To the greatest extent possible, I will set that dates for the public meetings at the beginning of the year to allow adequate time for you to plan ahead.

I'll also be looking for new ways to engage with you and will be soon soliciting for new committee members. We anticipate the publication of the Federal Register Notice by the end of May and any questions regarding the solicitation or the committee's business may be sent to the DPIAC Executive Director, Nicole Sanchez.

Again, thank you again for volunteering your time, your efforts, your talents, on behalf of the
public. Also thank you to the members of the public who have joined us for today's meeting. I look forward to hearing from you all.

I'll turn it back over to Ms. Sotto. Thank you.

CHAIRPERSON SOTTO: Thank you so much. We are, I think you can assume that every single member of the committee is just so excited to assist as you need. So we are at your disposal.

Let me ask if I may, for any comments from the committee members.

(No response.)

CHAIRPERSON SOTTO: Okay. All right, then let's move on. And if we could get please a briefing from the DPIAC Policy Subcommittee Chair Dennis Dayman. Dennis is going to be providing the committee with an update on the information sharing tasking, that that subcommittee has been working on for some time now.

MR. DAYMAN: Thank you Lisa. Can you hear me fine?

CHAIRPERSON SOTTO: Perfect. You're perfect.
* MR. DAYMAN: Awesome, wonderful. Well, thank you very much for that and welcome everybody. And I'm glad to see that we're back to work here within the DPIAC, and again, we welcome our new Chief Privacy Officer to the position.

Just as a quick update, you know, in terms of us filing, you know the update, pursuant if you guys recall, in October of 2020, we were tasked with creating a Policy Subcommittee to look at three different things really.

A lot of it was around how to provide guidance and best practices to ensure the effective implementation of any sort of privacy requirements that DHS would have around information sharing across the DHS enterprise, and also any sort of third parties or other government agencies, as well, that would come into contact with the data that would be required be transferred.

But more specifically how the Privacy Office could better engage with the other offices and other components to, you know, obviously improve the consistency in meeting any sort of requirements
on information sharing requirements. And again, the impacts on privacy positively or negatively.

And the secondarily to that, you know, how the Privacy Office could provide better oversight of those protections that are included in, you know also, information sharing agreements that DHS and other entities might have, and that were there any specific metrics or anything that could be utilized within those agreements and what the processes currently had been, could we find improvements to them and then moving forward what those improvements might look like.

And then third, were there any additional considerations necessary to implement those privacy requirements into those sharing activities.

You know, obviously 2020 was an interesting year for us in terms of a lot of things, but since that tasking took place, this subcommittee came together and met several times during the past administration and at least once during the new administration right now, and obviously during that time period some changes and some scheduling
issues, you know, had come up.

But during the first, sort of, you know meetings that we had this subcommittee, took a tasking if you will, internally, sort of, to understand how DHS departments handle and share information, again within DHS, other government agencies and then also outside of DHS. And during that time, we asked staff, several different requests I should say, to provide more guidance and other examples of even things like past memorandums of understanding or MOUs within DHS and third parties. So we, as a subcommittee, especially for some of us who had just gotten here in recent years could understand a little bit more about what had been -- what has been working. And again, you know, what areas do we think as a subcommittee and our experiences could be brought into this.

And then whether or not other things like the, you know, Federal Information Processing Standards baselines were being used and what those practices and policies, you know also look like.

And again just really sort of just getting a better
understanding over the last couple of years, what's
been required of the previous administrations and
staff as well.

The committee had also had requested other
clarifications as well, on whether or not the
tasking at the time -- when we looked at the
tasking as a subcommittee, there were a couple of
questions that had come up to get clarification on
to say, you know, were the three things, if you
will, that were that were given us as a tasking
correctly identified and detailed enough for us as
the committee to go through and figure out if any
sort of actions need to be taken correct or
incorrect, right?

And so, you know, in the early stages you
know we had felt that those taskings could be
lacking or may not be held enough for the committee
to take action on and again we went back and sort
of asked those questions.

There was also a request that was made to
staff by the subcommittee to have a better
understanding of the report that was issued on
November 4, 2020 which was the DHS Office of the Inspector General, or what we call the OIG 2106. And the title that was “DHS Privacy Office Needs to Improve Oversight of Department-wide Activities and Programs and Initiatives.”

And that was provided to the committee members and reviewed, you know, in our last meeting to understand again, you know what the recommendations, had been from another point of view, really.

And then last of all, you know, the committee had requested, again, additional sharing or Information Sharing and Access Agreements, or ISAAAs, to again understand what sort of partners and balances had been represented and types of data that have been asked for -- whether they were domestic, international, biographical, biometric, and other sorts of pieces to that. And again, staff had given us that task to review in the last meeting.

With these asks to the staff and those findings, the, you know, the committee again in our
last meeting in March, began to have a better understanding of what DHS is like for data sharing practices and discussions. And there were several things that we came out with and that we have filed back to DHS on, but I'll kind of get into some of the more details of some of these. And again, we are planning on reviewing these and understanding whether or not that these are the routes we want to take.

But things such as, you know, whether or not if a much larger council or data governance is still required and being maintained by DHS in the functional area so you know, should we consider reviewing or reviving an Information Sharing Council within DHS with Privacy as a member.

You know, things such as privacy practices within DHS as well, possibly looking at whether or not DHS needs more process versus policy in some areas, things such as, you know, getting a better understanding if existing policies were good enough for carrying out the mission, with or without data agreements in place at times, working to then
identify information categories that currently are
in place and what categories and types of
information are being shared. How much involvement
from each privacy office, you know, within DHS are
given or involvement are given, and also if proper
time has been allotted to review information
sharing requests, and how often are they allowed to
review past requests for changes in data use and
sharing?

And this would include again opposite the top
DHS Privacy officials in office as well, but making
sure the Privacy Office is provided an opportunity
to review, again, also all of the information
sharing agreements -- and there are quite a number
of them out there, to ensure that privacy
considerations are addressed for sharing, again,
information outside of DHS, whether federal state
or agency or foreign government.

And then also looking at also if better
communication practices are needed and required for
those data shares outside of DHS.

We also discussed quite a bit and made some
internal -- I guess recommendations to ourselves as
to whether a new data repository within a tracking
system or tracking system is still available and is
usable for the current taskings by DHS and
information sharing practices. And we want to
consider reviewing those information sharing data
bases as a clearinghouse to help also inventory
existing agreements and moving forward, new
agreements or information sharing agreements and
whether or not a reminder process if you will, for
a regular annual, biannual, whatever that needs to
be, review of these agreements, you know, would
happened.

And then more importantly, I think as you
look at all these sorts of things is what metrics
are being performed during the privacy impact
assessment review. You know when data is being
shared, for how long, how often are those PIAs and
agreements are being reviewed. And even, again, at
that renewal time period that I just mentioned and
whether or not those involved have the ability to
be notified when a PIA or data agreement is about
to expire, and needs to be re-reviewed moving forward to understand whether or not the information sharing practices and requirements are still being met or exceeded.

You know, within that establishment again, that repository, that also would send an alert to the Privacy Office when it's time to review those terms are approaching. Perhaps a three month period, you know, is something that could be looked at, and that we're considering as well. And then after which the agreements are auto-renewed if no objections are received, so that we're not stopping any critical data sharing agreements that could be related to, you know, to national security issues.

And then whether or not it would be in the best interest of DHS to stop data sharing of those processes, if those processes -- excuse me -- are not being followed. Again, if those data stoppages happen automatically, could they negatively affect those, again, national security data sharing needs?

And then the last few things to those would be also then how can the process ensure that
privacy receive a timely opportunity for input as well? You know, can we incentivize -- can an incentivized system be created within DHS and within the agencies that work with DHS and are there any risks that can be identified for the owners to help incentivize them as well to want to, you know, ensure that their agreements are in place that they're properly being maintained, and again, if they're doing the privacy impact assessments.

And then what failures could -- you know, if a failure happened for a proper privacy review, you know, would there be any sort of, you know, things that we could be doing there as well.

And then last again, can an existing process that requires the Privacy Office review be leveraged to ensure a review. So an example of that would be a PIA is required for a system, you know, could that PIA requirements around information sharing be strengthened to require documentation of say data flows and MOUs and MLAs.

So with those findings in mind Lisa, you know, the subcommittee is getting ready to explore
those potential avenues for further review and develop more specific recommendations for the committee's consideration -- for the overall committee’s consideration. I know that I have already had the pleasure of having a one-on-one with Lynn Parker Dupree, just a few short weeks ago, and we've also asked her to provide -- well, we provided her an opportunity to provide further direction or related requests to the original tasking, if so desired by her.

And again the subcommittee is looking forward to DPIAC’s public review meeting today and if there's any questions that might come from our current committee or the public as well. And with those thoughts and findings in mind, again we're looking forward to the work that's going to come from this.

CHAIRPERSON SOTTO: Dennis, thank you very much. You have a very big remit here with this tasking. I have a question, I'll just start off. And you mentioned this, I just would be interested in hearing a little bit more about it. So it seems
to me that sort of a baseline for understanding this issue generally is to have a good repository of information sharing agreements and an inventory, you know, table of contents if you will, with maybe a chart and summary.

This is, you know, really lay terms of how to keep track of things, but I'd be very interested in hearing if there is that sort of repository and inventory. And then, it's not different -- a second question, really not that related is, is there any kind of documentation around guardrails for information sharing, either within the Department or outside Department?

MR. DAYMAN: Yeah, so I'll start with the latter really quickly because that's a that's a quicker answer. But yes, there are guardrails currently that are out there.

I think as the committee and staff have looked at what those processes look like, you know the guardrails that are currently there are not quite completely outdated by any means, but you know as DHS, itself, has grown as an organization
in different aspects, different agencies under DHS and the uses of data that have been needed over time, you know, looking at those guardrails again, we think would be beneficial for us to understand again, you know, the original ask or the original intention -- excuse me, of the data request, right? The data sharing, you know, is it still the same need and you know, is potentially additional data might be, you know, given out over time outside of those guardrails.

We have not been able to identify that just yet to-date as we're still kind of in its infancy, and looking at those, but there have been some questions as to whether or not that, you know some of the data that's there needs to be re-reviewed to make sure that it hasn't gone any further beyond what the original agreement was.

The first question though, around that system, yes a system does exist, it is one again that was an early onset system. But over time, again as DHS has grown and staff and agency aspects or how things report up into up in the DHS have
changed. It really hasn't been maintained as well, I think from what we understand at a very high level, and that it kind of needs to come back and be a lot more centralized for DHS in a sense, because again there's a lot of different Chief Privacy officers that are out there within DHS.

And each one of them also has a different need and a different requirement, and a different sensitivity as well to that data and some of the questions that have come up as to, again, say has this system that's been out for this repository system grown with, again, the task as DHS overall? And should we be looking at improving that?

Again, getting all that input from all the different agencies as to how they would use that and how they would interact with it because it's a little bit different for everybody at times.

CHAIRPERSON SOTTO: Thank you very much.
Others? Am I missing a raised hand Nicole?

MS. SANCHEZ: I don’t see any raised hands.

CHAIRPERSON SOTTO: Okay, all right. So we’re good.
Dennis and committee members, subcommittee members, thank you very, very much. This is a really big topic and it's such an important topic. Lynn, I think did you have something that you wanted to add?

MS. PARKER DUPREE: I did. I just had a quick question and you may not have gotten there yet. But have you identified any sort of categories of information sharing that might be useful to sort of use as a prioritization matter?

MR. DAYMAN: No, we have not yet.

MS. PARKER DUPREE: Thank you.

CHAIRPERSON SOTTO: All right. Anything else to add on that point?

(No response.)

CHAIRPERSON SOTTO: Okay. Do any of the subcommittee members want to add anything?

(No response.)

CHAIRPERSON SOTTO: All right, good to go then.

Dennis and subcommittee, thank you, thank you. We really appreciate your work on this.
There's a lot, a lot to be done and it's such an important project.

So if there are no more questions for Dennis or the subcommittee, I'd like to turn it over to the Emerging Technologies Subcommittee, and its Chairperson Chris Teitzel for their tasking update.

Take it away Chris.

* MR. TEITZEL: Thank you Lisa. Thank you.

So as a quick recap here, our tasking was to consider the Department of Homeland Security’s transition to cloud service technologies enhanced capabilities that have happened during the transition due to COVID-19 to the telework environment, and to determine if there's any associated privacy risks that would merit near-term tasking from that.

As a quick background during our last meeting, we were provided information from former Chief Information Officer Karen Evans and she provided us information about that transition. So the transition happened almost overnight, as we all know in the March timeframe last year. And the
Department went from an average daily load of 10,000 teleworkers to 70,000 almost overnight. And in addition to the 7x that we saw in telework, the Homeland Security Information Network saw a 200 percent increase, and the VPN for the DHS saw a increase by 483 percent.

Any one who has worked in IT or networking, knows the stress that this can cause, as you have so much happening so quickly and moving so fast. But luckily, the Department was actually fairly prepared for this and we found this out as we were conducting an interview with a member of the OCIO, the Office of the Chief Information Officer.

And they said that in 2018 and 2019 there were large snowstorms that forced a large number of DHS employees into teleworking, and because of that, because of the snowstorms that occurred in years prior, the use of cloud tools, the Microsoft Office Suite Teams -- which we’re on now, started becoming more and more prevalent and started being used more and more. And so, we actually have a front run on the pandemic and this migration.
And so, though a large transition occurred, it seemed to go as smoothly as one can imagine and actually from the subcommittee's viewpoint, it actually has gone incredibly smoothly.

This migration has also been conducted side-by-side with a larger migration to the cloud, off of on-prem servers and on-prem data centers. And so, that movement is to -- obviously with the cloud we can improve service availability, reliability, be a bit more cost effective in that server utilization and data center utilization. And so it's a three-pronged effort that they're going through, still currently.

And the three prongs are the migration of data services, and computing to the cloud wherever possible, the consolidation of data center operations. So now that we're moving more and more into the cloud, can we consolidate our existing data centers into more centralized areas that are easier to manage and easier to oversee?

And then those that do remain in on-premises data centers, can we modernize them? As we're
moving into the cloud and able to have better virtualization and server utilization technology, can that also be applied to the on-prem data centers as well?

And so, in our conversations with the OCIO’s office we saw that, currently, all systems have been accounted for and identified, which is, as one can imagine for a department of our size, a large tasking in and of itself, and again, because this has started years prior, this process is currently underway and was already underway when the pandemic hit.

And so, not only were they accounted for and identified, they each also have gone through an evaluation to see if it's able to move to the cloud. Some systems are not and that's valid. And then, if not, we need to have justification written up and for why it's staying on-prem. So that way we're not just leaving systems on-prem for the sake of it, we're actually providing justification and going through a qualification process there.

And then additionally, those legacy systems
are being rebuilt with modern technology. And, you
know, trying to get to as close to par as we can
with their cloud counterparts for resilience and
security as well.

So as we move, you know, as a department into
the cloud, there's quite a bit of risk there as we
all know, especially from a privacy perspective.
And we wanted to look at a few items as a
subcommittee in our questioning with the OCIO’s
office around this. The first one being data
security, that's kind of the more obvious one, the
one that everyone thinks about. Is that, you know,
are we making sure that the new systems are set up
with the proper permission and sharing to make sure
that access to data is maintained, and there's no
leakage -- data leakage in the process into an
insecure system.

The second one is integrity, data integrity.
And this can often be overlooked or understated
during migrations, but it's important to make sure
that as data is in motion, as it's moving from the
on-prem into the cloud, that we ensure that there's
no loss, that there's not an incomplete transfer, that temporary storage locations aren't left open. And there's a great deal of consideration that can come from just maintaining integrity in that process. And I'll get into here in a minute the steps that are being taken for that.

And then lastly, is obviously what we're here for, and part of the committee's tasking is the privacy of it and making sure that as we're moving data are we finding personally identifiable information PII, in that movement? Are we identifying new data that needs to be protected? And how does that get managed, how does that get identified, and then eventually how does it stay secure?

And so, in our conversations with the OCIO's office, we were given a quite a large background on their process and the steps and the audits that are in place. There's audits that take place at the outset, during the migration, and then post-migration to ensure that all steps and all procedures have been followed and all data has been
secured and remains private as necessary.

We were given access to Homeland Security's 4300A Handbook, which is kind of the overarching policy document that governs all the data security and privacy within the department. And then, augmenting that our management directives, which give more coverage to more modern technologies. So the Systems Handbook is a large handbook, it doesn't get rewritten nearly as often. The management directors are there to augment that, and there's even addendums to the management directives which are more modern and applicable. So there are kind of tiers to how the procedures and policies are in place for, as well as removing systems and classifying systems where the data sits and how.

And so we looked at those, and we also looked at kind of a general overview of directives within the system. And, you know we're awaiting word from the Office of the Inspector General to understand more about the cadence of post-migration audits, and how often those are occurring. We want to make sure that as we as we look at data -- okay, it's
been moved into the cloud, we're where we want to be and we've hit all the milestones. A year from now, two years from now, what's that cadence look like? To come back and check. Are the systems still acting as they should, and are they still secure and private as they should be?

So we're awaiting for that information but in the meantime, we've been as a committee, meeting and working on some recommended next steps. We're putting those in together into a formal recommendation and kind of tasking report that will be sent around to the subcommittee, first for review and then to the larger committee and then eventually to the Privacy Office as well.

And so, I can give a kind of an insight into where we're leaning towards and our recommended next steps. We don't see any immediate taskings coming out of this. I think our overview has been, or at least immediate taskings for the subcommittee. I don't think that we have found anything glaring -- and this is a very good thing. We haven't found anything glaring that needs our
immediate attention.

There are some issues that we're wanting to look into with more modern cloud technology. As we all know policy moves slower than technology. And so as we're adopting more and more modern technologies and more and more modern cloud architecture, if there isn't a management directive for that, and there isn't an addendum that covers it. The Office, the OCIO, falls back to working with the technology partner or software creator, in order to build out according to best practices. It would be good for us to look at how can we internalize those into future directives and in future addendums just to cover new technology that comes in.

Secondly, as I talked about. We're looking at the OIG’s cadence and what those ongoing audits look like to make sure, as we know, just because something got moved at the outset in a proper manner, sometimes controls can break down over time. And so, we want to make sure that that audit process happens at a regular pace.
And then lastly, we're working up some
guidance around ensuring just as it occurred during
this process, but also just in a more general
sense, that privacy by design principles can be
implemented in future undertakings like this. And
so making sure that policy and technology, have a
seat at the table at the beginning of the process
in order to ensure that that privacy and security
continues, and not just a checkbox in the audit at
the end where, you know, it may be too late or it
may be overly burdensome or costly to then go back
and rectify any mistakes that occurred.

So those are the three steps that we're going
through now. I anticipate that report being
wrapped up here shortly, and then we'll be
submitting it around to the rest of the committee
once it's ready.

CHAIRPERSON SOTTO: Thank you very much.

Thank you to both subcommittee chairs for really
very thorough explanations of what you're doing.

Let me open this up to questions from the larger
committee. Does anyone have questions?

(No response.)

CHAIRPERSON SOTTO: Okay. No questions. So, Chris, I just want to, I think to just clarify. So we're finding that we do not need a larger tasking on this, but we are going to issue as a full committee, a short statement or report, whatever we call this paper, summarizing your findings and maybe making a few recommendations directly rather than taking on another tasking. Is that accurate?

MR. TEITZEL: Yeah, that's correct. At this time I don't think the committee's found any immediate taskings that that would be under our purview to take on.

CHAIRPERSON SOTTO: Okay, perfect. And Lynn can tell us if there's something that comes out of this particular exercise and that she'd like us to take on as a subsequent exercise. So good.

MR. TEITZEL: Yes, thank you. And, again, to highlight here in a public setting the efforts that the OCIO’s office has gone through in the past, you know, 13 months now, 14 months. Has been nothing
short of a miracle. So, you know, kudos to them and all the hard work that they continue to do in this process.

* CHAIRPERSON SOTTO: That's great. That's a great shout out. Thank you. That's very nice. All right. Well, if there were no more questions for Chris or the subcommittee, I'd like to begin the public comment portion of our meeting. So there were no pre-registrants with respect to comments. So I'd like to open the floor to any members of the public who wish to speak and I would ask that you please keep your remarks to about three minutes, as was described in the Federal Register notice. So if you're joining by phone you can mute and unmute by pressing star-six.

(No response.)

CHAIRPERSON SOTTO: All right, a quiet bunch.

MS. SANCHEZ: Lisa, this is Nicole. I want to jump in just a second because we did receive late-breaking comments from Jake Weiner from EPIC, and so I just wanted to see if he was able to join us.
MS. SANCHEZ: I don't think so.

CHAIRPERSON SOTTO: Nicole, do you want to read, I don't know what the format was and whether it's appropriate, but if you'd like to read that to us.

MS. SANCHEZ: I can't, it's about nine pages.

They will be posted on the website.

CHAIRPERSON SOTTO: Perfect. Nine pages is not readable on a Zoom call or a Teams call.

Okay, good. So we'll post that and certainly take the comments under advisement, so thank you for that. Of course any written comments are treated as public documents and are available for public inspection, so good.

All right. Well then, with nothing further I think this concludes our public comment period.

I'll just pause for five more seconds.

(No response.)

* CHAIRPERSON SOTTO: All right. I will then go ahead and close the public comment portion.

Again if you if you would like to submit
written comments please do. We would really welcome them and you can email them to “Privacy Committee@hq.dhs.gov” And if you could do so by May 28th, we would appreciate that.

And with that, many thanks to our speakers, our committee members, who really have worked hard on these taskings and you can see by the amount of work that's been done that these issues have been well considered.

We thank members of the public for participating as well today.

This formally concludes today's public meeting. We are grateful for your interest and we would encourage you to follow the committee's work by checking our webpage. The minutes of this meeting will be posted there in short order. And with that, this meeting is formally adjourned.

Thank you very much.

(Whereupon, at 1:43 p.m., the meeting of the Data Privacy and Integrity Advisory Committee was adjourned.)