1

UNITED STATES GOVERNMENT PRINTING OFFICE

DOCUMENT AUTHENTICATION WORKSHOP

Friday, June 18, 2010

732 North Capitol St., NW

Washington, D.C.

9:10 a.m.

```
 1                P R O C E E D I N G S

 2           MR. HANNAN:  Welcome everybody.  Thanks for

 3  coming today to our workshop on Document

 4  Authentication.  I'm John Hannan from GPO.  I want to

 5  extend a welcome to you.  I haven't met everybody but

 6  thanks for making time today.  We really looked forward

 7  to this.

 8           Just a couple housekeeping things to get

 9  started with.  There are restrooms right down the hall

10  on your left as you go out -- straight out this door,

11  on the left.  I think the men's room is first on the

12  left.

13           We have a transcriber here today, as is often

14  the case at the library conferences, and so later on

15  when we have opportunities for feedback, we have three

16  handheld mics that we'll pass around the room.  If

17  you'll please wait for a mic and if you'll pass the mic

18  around and then if you'll state your name and what your

19  organization is, that will help with that.  And we'll

20  post the transcription later on at the end of -- about

21  a week from now, just five to ten business days

22  (inaudible).  We'll plan to post that for folks.
```

1   Lunch, around 11:45 we'll probably break for

2   lunch and that will be on your own. Since the GPO

3   cafeteria is available we'll show you how to get over

4   there to get some lunch. And then we'll reconvene at

5   one o'clock to get started for the afternoon session.

6   So -- and we have a break in the morning and break in

7   the afternoon.

8   Unfortunately we don't have wireless in the

9   room here, we're working on that but it's not ready yet

10 so our apologizes on that. But there are plug ups for

11 your laptop if you want to run your laptop.

12   I'm thinking here, Lance did I miss anything?

13   MALE VOICE: I don't think so.

14   MR. HANNAN: Okay. Oh, and everybody looks

15 like they've turned their tent cards around so that

16 folks can see and the transcriber can see, that would

17 be great. I'm going through my checklist that Lance

18 gave to me, I think I'm on track here so far.

19   There's a handout from you which are all the

20 slides. They're up here too and we'll kind of step

21 through that. They're mostly to provide some

22 background and give us some guide to help bring some

1 feedback from you all for some questions and some

2 topics that we'd like to hear what you all think about

3 these things, as we talk about some of the finer points

4 of document authentication as we look into the future

5 here at GPO. We really appreciate you being here to

6 give us some insight and some thoughts.

7   So before we get started, thank you, we'll go

8 around the room and just do a quick introduction for

9 everybody. We will go ahead and give everybody --

10 after the conference we'll provide a list of who was

11 here and we have a website link, it's at the end of

12 your handouts -- where things will be posted later on

13 about our workshops and things.

14   So with Lances help, I'm John Hannan from

15 GPO, I'm the Chief Information Security Officer at GPO

16 and I have a long, pretty long by now background in

17 data integrity and electronic authentication. Since

18 I've been at GPO about six years now I've been working

19 with people on authentication. It's been really

20 exciting and a pretty fun initiative overall to be able

21 to bring some capabilities to the table (inaudible).

22 So that's me and we'll go around to my left.

1   MR. SMITH: I'm Steven Smith. I work with

2 GPO for John Hannan. And I support the PKI

3 Instruction.

4   MR. WASH: I'm Mike Wash, I'm an IT here at

5 the Government Printing Office. I'd just like to thank

6 everybody for coming. As you know, authentication is

7 one of our foundational aspects in our content

8 management activities that we've been working on for

9 the last six years in our federal digital system. And

10 as we positioned, you know, early on, when we were you

11 know, conceptualizing this system, we realized that

12 authentication was going to be a journey.

13   We have tools today, using Adobe Live Cycle

14 that allows us to digitally signed PDFs, as you all I'm

15 sure are well aware. But it really isn't enough. There

16 are new format types that are coming available that

17 people would like to have signed or in some way capable

18 of being authenticated for their use and we've got to

19 find solutions for that. Plus a lot of the documents

20 that we sign today are very large and subsets of those

21 documents would be nice to have signed as well or

22 authenticated. So a lot of our discussion today is

1 really to help us understand, from your perspective,

2 what some of the real value propositions are for

3 authentication and what the requirements would be for

4 authentication so that we can frame it properly as we

5 continue to move on this journey.

6   Later this year we expect to have, and I'm

7 probably taking some of your thunder here, John, but

8 later this year we expect to have more of one of our

9 technical work sessions which we call an Industry Day.

10 And an Industry Day is where we bring the supplier

11 community in to hear our story about what we think is

12 needed so that they can feedback to us and tell us how

13 they think they could help us solve their problems. So

14 this session is really to help us prepare for that,

15 because the last thing we want to do is have a room

16 full of sales people telling us they have the greatest

17 solution since sliced bread, which they all like to do.

18 Instead we like to be able to position what we believe

19 is the opportunity set and the value proposition we

20 need to deliver so that we can really help manage those

21 future conversations to be as effective as possible to

22 provide solutions that will ultimately meet everyone's

1 needs.

2   So again, thank you all for coming. I think

3 it's going to be a good session. I really appreciate

4 your support with this.

5   MS. SEARS: Suzanne Sears from the University

6 of North Texas. And I'm here representing the Federal

7 Depository Library Council.

8   MR. PRIEBE: Ted Priebe, GPO. I'm with the

9 Library Services Business Unit. I work for Rick Davis.

10 Our unit collaborates with the content originators in

11 terms of getting their support to authenticate

12 collections that ultimately will flow into FDSYS, the

13 Federal Digital System. Thanks for attending.

14   MS. BAISH: Mary Alice Baish, I'm the

15 Director of Government Relations for the American

16 Association of Law Libraries and obviously the issues

17 of electronic life cycle management, permanent access,

18 authentication, official status, preservation are key

19 components for our community, particularly as we all

20 know, when the official titles are disappearing.

21   So I would like to thank GPO on behalf of our

22 organization for holding today's event. And also I'm

1 very excited that it will be followed up by an industry

2 event.

3   MR. YU: I'm Harlan Yu, I'm a graduate

4 student in computer science at Princeton University.

5 And for the time being I'm at the Department of Labor

6 working (inaudible).

7   MR. BOOTH: My name's Harold Booth. I'm a

8 computer scientist at the National Institute of

9 Standards and Technology in the Computer Security

10 Division.

11   MS. CASE: Pat Case, I work with the

12 Congressional Research Service and I work on LIS which

13 is the Hill version of THOMAS.loc.gov.

14   MS. MCGILVRAY: Jessica McGilvray, I'm the

15 Assistant Director at the Office of Government

16 Relations at the American Library Association.

17   MR. GEE: Robert Gee with the Law Library of

18 Congress, primarily working with THOMAS. I'm also

19 doing some utilization initiatives with GPO.

20   MR. COGGINS: I'm Tim Coggins, I'm the

21 Associate Dean for Library Information Services at the

22 University of Richmond School of Law and have been with

1 the American Association of Law Libraries efforts

2 (inaudible).

3   MS. DULABAHN: I'm Beth Dulabahn for the

4 Library of Congress and I'm involved with their

5 digitization programs and the actually digital

6 information infrastructure and preservation program.

7   MR. ANDERSON: Which is N-DIP (ph) for short.

8 I'm Steve Anderson, I'm the Director of the Maryland

9 State Law Library in Annapolis. And like Tim I've been

10 working with the American Association of Law Libraries

11 tracking authentication issues for some time.

12   Also, this year in Maryland we did -- well

13 over the past couple of years we've had the occasion to

14 try to find out what some best practices are for

15 authentication for state publications. Our state

16 publications depository and distribution program needs

17 to have some guidance at some point, in my opinion. And

18 we were faced with almost eliminating the print version

19 of the Maryland Register, our federal register

20 equivalent, which did not happen fortunately, but there

21 was no Plan B in terms of authenticating any of this.

22 So to the extent that there's some possibilities of

1 cross pollination that would be fantastic for me to

2 pick up.

3   Lastly, on a personal note, I've got young

4 onset Parkinson's Disease so if you see me shake a

5 little bit or something like that, just pretend I'm

6 Michael J. Fox and I'm being famous. Thank you.

7   MR. TAOULTSIDES: I'm George Taoultsides

8 Research Librarian at Harvard Law School Library.

9   MS. ZWAARD: Hi, I'm Kate Zwaard, I work at

10 GPO and I work on the Federal Digital System

11 responsible for the digital preservation component

12 which includes content integrity and (inaudible).

13   MR. HORTON: I'm Bob Horton from the

14 Minnesota Historical Society. I'm the happy recipient

15 of an N- DIP (ph) grant to work with the preservation -

16 - long term preservation of digital content from state

17 legislatures and I'm an observer for the Society of

18 American Archivists on the National Conference of

19 Commissioners Uniform State Laws Task Force for

20 (inaudible) Law on Authentication and Preservation,

21 religious related or legal -- digital legal documents.

22 Is that what they're calling it?

1   MS. RUSSELL: I'm Lisa Russell from GPO. I'm

2 the Library Services and Content Management Division

3 and I've been working on the authentication initiatives

4 for a few years now.

5   MR. WEBER: I'm Andrew Weber at the Law

6 Library and the Library of Congress and I work a lot on

7 THOMAS.

8   MR. SHULER: John Shuler from the University

9 of Illinois at Chicago. I'm also a member of the

10 Federal Repository Library Council.

11   MR. GALLUCCHIO: Kevin Gallucchio, Department

12 of Defense. I'm supposed to be some sort of subject

13 matter expert with XML.

14   MR. MAYER: I'm Jonathan Mayer, I'm a fellow

15 at The Center for Computers and Law at Stanford and a

16 graduate student in computer science and law.

17   MS. LAPLANT: I'm Lisa LaPlant from GPO. I'm

18 in the Program Management Office and I work primarily

19 on the access and delivery and search portion of FDsys.

20   MS. DALECKY: I am Selene Dalecky. I am also

21 in the Program Management Office here at GPO. And I'm

22 the FDsys program manager.

1   MR. DAVIS: My name is Rick Davis I'm the

2 Acting Superintendent of Documents at GPO. I'm also

3 the director of the Library Business Unit that manages

4 the FBLD (ph).

5   I want to thank all of you as well for coming

6 this morning and give a little bit of background as

7 well as to add to what Mike mentioned earlier. Back in

8 about 2005 the Deputy Public Printer at the time

9 approached me and said, "You know, we've got a growing

10 crisis with digital documents and ensuring their

11 authenticity. We need to stand up a PKI." So being a

12 policy person and nontechnical person, the first thing

13 I did was go to a library and say, "Well what is PKI

14 all about?" Well from there, working with John Hannan,

15 our IT staff, you know, here we are today.

16   We're now in an environment that many of you

17 see where in the federal sector over 95 percent of all

18 the new publications that come through us, that we make

19 available to the Federal Depository Libraries are

20 digital. In some cases not only are born digital but

21 there is no print equivalent. In a primarily print

22 based environment, when the Superintendent of Documents

1 sent out government publications sealed in a tied back

2 environment, there was a reasonable assurance that the

3 recipient, whether it was a sales customer buying our

4 product or a library receiving it, had a reasonable

5 assurance that they were actually getting an official

6 and authentic federal publication.

7   The challenge that we're now facing is when a

8 publication is made available digitally from GPO or

9 another agency and is indexed and Googled and picked

10 off on a number of other sites, how does the user, how

11 does the American public, the researcher know what

12 version to cite for -- in terms of being the official

13 and authentic version.

14   And we started addressing that issue by

15 applying digital signatures to our content with GPO

16 Access. It's now been expanded through our federal

17 digital system. But I think that, you know, part of

18 what we'll discuss today are some of the additional

19 challenges that we have going forward in this

20 environment dealing with levels of authentication, not

21 only for born digital content, but as we work with

22 digitized content, tracing back a chain of custody and

14

1 what chain of custody really means for different

2 levels. Likewise, looking at granular levels of

3 authentication that John's going to talk in more detail

4 about.

5   We have users who are saying, "It's just not

6 enough to authenticate an entire file that encapsulates

7 the publication. We want to be able to take snippets

8 of information from that publication and have the

9 authentication carry forward for additional needs." So

10 these are some of the challenges that we're going to be

11 facing. And again, I thank all of you for being here

12 and look forward to the discussion.

13   MR. SCHWEICKHART: Good morning, my name is

14 Reynold Schweickhart I'm the Acting Chief of Staff and

15 the Chief Technology Officer. On behalf of the Public

16 Printer and also the fifth person to welcome you today.

17 This is an important workshop to continue the progress

18 we've been making as we look at GPO's historical

19 mission to really provide authenticated government

20 information which we've been doing in the repository

21 library program since 1813.

22   On a personal note I've been working in this

15

1 space since I came to work for Congress and we worked

2 closely with GPO and the Library of Congress and CRS,

3 including THOMAS. And I also helped form the working

4 group that began the migration of legislative data into

5 XML which was now many years ago. So I'm excited to be

6 here. I think this will be a very productive day and

7 look forward to engaging with everyone.

8   Let me just go back and -- we've been going

9 around and introducing ourselves Daniel, so let's pick

10 you pick up here.

11   MR. BENNETT: All right. I'm Daniel Bennett

12 with the eCitizen Foundation. And we have worked with

13 the folks at the House and the House administration on

14 efforts to look at XML for these legislative documents.

15

16   MR. SHAPIRO: I'm Arin Shapiro the webmaster

17 for the Senate. I manage the central portion of

18 Senate.gov along with several intranets. I work with a

19 lot of the agencies here on a bunch of issues.

20   MR. HANNAN: Jim, why don't we go around and

21 start with you on the folks or let's actually

22 (inaudible).

1   MS. COOKS: I'm Judy Vance-Cooks (ph),

2 Managing Director for Publication and Information

3 (inaudible).

4   MR. BENDER: Jim Bender, I work in the

5 Production and Engineering Division of Plan Operations

6 and we primarily (inaudible) various GPO publications

7 such as the Congressional Record and the Federal

8 Register and some of the different legislative work

9 that comes down from Congress.

10   MR. GREEN: My name is Lyle Green, I work in

11 the Office of the Congressional Publishing Service at

12 the GPO. My office serves as liaison between GPO and

13 Congress.

14   MS. SWIATEK: My name is Kathleen Swiatek

15 (ph) I'm a IP Specialist in Congressional Support at

16 GPO. And I primarily work on XML projects on

17 congressional publication bills and we're starting to

18 report some other documents also.

19   MR. KAUFFMAN: My name's Mark Kauffman, I'm

20 from GPO. I work for Mr. Wash in IT and I'm the

21 Project Manager for GPO's (inaudible).

22   MS. SABOL: Hi, I'm Janice Sabol, I work in

1 Planning and Development in Library Services and

2 Content Management.

3   MR. HANNAN: Great. Well I think we'll go

4 ahead and get started. I believe I mentioned there are

5 some handheld mics so when it comes time and you'd like

6 to provide some input and speak, if you'll please turn

7 it on and state your name and who you're with. And if

8 folks would help by passing that around that will

9 probably be good.

10   So with that we'll go ahead and get into it

11 and what we'll do is, this is the agenda for today,

12 kind of a guide for discussion. We've obviously been

13 through the first part.

14   Authentication background, individuals as

15 well as for automated high volume uses. Standards and

16 methods, we're going to spend a lot of time this

17 morning on standards and methods because that's an area

18 where we'd like a lot of input. And we have some

19 questions, we have some thoughts but also some

20 questions. When we come back from lunch we'll go into

21 chain of custody, type of use cases, re-authentication

22 over time. That's really more just just awareness for

1 you more so than input, I think, but we're here to

2 listen. So we look forward to that. And then lastly,

3 granular authentication and then we'll wrap up.

4   A little bit about what's in the scope for

5 today, what's out of scope just because we don't have

6 that much time really for some of these topics. We're

7 really talking and want to focus on authentication for

8 the electronic documents that we've assembled at GPO.

9 What we don't want to spend time on today is

10 authentication as we might apply it to tangible or

11 other products at GPO (inaudible).

12   A little bit about what we're thinking in

13 terms of the desired outcome. Really we said this a

14 little bit but, the next slide was a slide for your

15 handout, we'd like to get feedback from the various

16 stakeholder constituencies we have here to help inform

17 our decisions that we're going to have to make about

18 future system deployments. You know, we don't lack for

19 a lot of different ideas or methods, what we really are

20 looking for is to see if there's some consensus that

21 will help us make our decision about how to provide the

22 best value for citizens and all of our constituencies

1 here today. And as Mike said earlier, this will help

2 us form the input for the follow on industry data that

3 we will have. We'll be asking parties about what kind

4 of technical and other systems they might provide to

5 help us in that regard.

6   So some of the decision topics for today, the

7 first one is does the community really require

8 different levels of authentication assurance on the

9 same content. Some parties are willing to use a les

10 robust means and others requiring the current digital

11 signature, is that really something that's important or

12 not? It's obviously more complicated and expensive for

13 GPO to do, but this is the area of feedback that we'll

14 get in to that we think is important and want to hear

15 from you on.

16   Next we all know XML is a very important

17 format. We're already publishing or disseminating

18 rather information in XML format. What standards and

19 techniques ought we to use for that format. Again,

20 there's a few different ways to go with that and we'd

21 like to get some input and your thoughts on that.

22   And what techniques and standards ought to be

20

1 applied to chain of custody? There's a lot of

2 different ways to go with that. Again, one of the big

3 things in this regard too is content originators really

4 need to support the electronic dissemination of that to

5 some degree. We can't make that call, I think, on our

6 own at GPO. So there's more about this as we get down

7 there, but that's an area we'd like to get some

8 feedback.

9   And then lastly, granular authentication.

10 We'll define what that is or scope it at least, for the

11 purposes of our discussion today. It could be many

12 different things. Some areas maybe not as concerned,

13 others very concerned with that, so.

14   Am I speaking loud enough for the -- okay,

15 good. Most people say I'm loud, so.

16   Some background on authentication. As you

17 probably know, we're publishing or disseminating PDF

18 files that are digitally signed using encryptographic

19 digital signature in PKI, and that's a specific kind of

20 method to use. That method uses an open international

21 standard that's really available for all parties to

22 write software code to do. And PDF is the standard as

1 well, again that people are free to write software

2 codes to process that kind of information.

3   As we go forward you're going to see those

4 are a couple of key points in all, from our

5 perspective, in all that we do. Not having proprietary

6 methods rather having open, international standard

7 methods that are available to all parties to use.

8 There's some other features as well.

9   For this we've gotten mostly positive

10 feedback from the stakeholder communities, at least

11 that I'm aware of working and talking with Rick and his

12 teams and Mike and their teams and everyone. I'm not

13 quite as close to all of your communities as Rick and

14 his team and Mike are, but I think generally that's

15 gone pretty well and we're really gratified. We hope

16 that that's provided some value to you.

17   That's been, from our experience, pretty easy

18 and reliable for users and citizens to really achieve,

19 knowing they have the electronic versions that came

20 from GPO. And if somebody tried to insert one,

21 purported to be from GPO, you could detect that easily

22 anywhere on the planet. So that's been our experience

1 so far. And again as Mike said, in the first step on

2 our journey with PDF that's been our experience so far,

3 but there's a lot more to it, since we think about

4 other content types and such.

5   Again a little bit more about the background.

6 We started off in 2008 actually with the President's

7 budget on GPO Access. You all probably know most of

8 this, so I'll go through it really quickly.

9 Congressional bills we started in the 110th Congress

10 with Rick's and Ruth and Lisa and we've a lot of our

11 folks working on that. FDsys data started, it's been

12 doing signing from the get-go in the Federal Digital

13 System or FDsys as we like to use the acronym here at

14 GPO, signing all the collections as the collections are

15 disseminated, the PDF files with digital signatures are

16 available.

17   So our goals, what are our goals as we see

18 them for authentication? This is to provide recipients

19 of documents or readers of documents with who the

20 source or disseminator of the document was. GPO is the

21 source for the GPO documents. Going back to what Rick

22 said, as trying to provide some value to a larger

1 community in reducing confusion about what did GPO

2 disseminate, kind of the definitive way to deal with

3 that in an electronic, faceless Internet-oriented

4 world.

5   Second bullet there, providing some assurance

6 that as you're reading the document it hasn't been

7 altered since GPO put it up on the Internet. So it's

8 also a means of reliably detecting, quickly and easily

9 for users, if it was altered. So that's a goal for

10 authentication programs.

11   And then lately to provide a method that

12 supports authentic chain of custody so that the chain

13 of custody can be reliably provided not altered as it

14 leaves GPO. And again, a way to reliably detect if it

15 was altered. This is obviously something that's

16 further down the journey for us and one of the reasons

17 we're having today's session (inaudible) about that.

18   So at kind of a high level those are the

19 three high level business and function goals we're

20 trying to achieve.

21   Okay, some factors that seem important to us

22 about how we take the next steps on this journey. We

1 want to use authentication techniques that are strong

2 enough to maximize the length of time the authentic

3 technique is valid. In other words, we don't want to

4 pick a technique that turns out to be so weak that we

5 have to go back or redo it next year. That kind of

6 wastes everybody's time, or mostly ours. And that's

7 not a good thing.

8   Authentication techniques that work even when

9 you're disconnected from the Internet. That's

10 obviously really good technique but those are the the

11 kind we'd like if we could get them. There are plenty

12 of techniques that require you to be connected to the

13 Internet, but it also works when you're disconnected

14 from the Internet, we think that's valuable but we'd

15 like to get some input on just how valuable that is as

16 such.

17   Authentication techniques are based on open,

18 published, established international standards as

19 opposed to proprietary method. That's obviously a key

20 question. Authentication techniques that are based on

21 binary data or open data formats rather than

22 proprietary data forms, that's what that last bullet's

1 really about, open, freely available formats not

2 proprietary formats.

3   Authentication technique that provides a

4 clear and simple display of who the disseminator of the

5 document was, not some convoluted technique or

6 requirement for 17 different mouse clicks but hopefully

7 something a little simpler. Again, some techniques that

8 they really, for a data format, require a lot of

9 complexity, well -- but we're going to look to and

10 guide -- our decision thinking is guided towards

11 simplicity where it's possible to still achieve the

12 other goals.

13   And then lastly, a technique that's

14 extensible for chain of custody. In other words not

15 something that we necessarily need to do at the

16 beginning but something that's easily extensible if we

17 want to do that, either from the start or later on down

18 the road.

19   So those were, to us as we talked about that

20 at GPO, some things that seemed like some of the

21 overarching principles. So at this point we wanted to

22 kind of stop and see if that makes sense or if there

1 are others that you think we should be considering too

2 in that regard. So I guess at this point we'd like to

3 go ahead and open it up for some feedback or some

4 thought process or thoughts from others.

5   That mic over the in corner, Harold, that's

6 the one mic where you have to press and hold the button

7 for it to go green, so -- okay, you've already figured

8 it out. Great. Thank you. The other mic has a little

9 on/off power switch at the top and you flip it to

10 power.

11   Again kind of a little abstract topics there

12 but those seemed like the criteria that we ought to be

13 looking at. Are there others that come to mind? If

14 not we can just move on into and get a little more

15 specific about some of the topics. And you'll have

16 plenty of time to send us feedback too after the

17 conference, by the way.

18   Yes, Mary Alice?

19   MS. BAISH: Just one quick question.

20   MR. HANNAN: And if you'll just -- it should

21 be -- I think it's on already.

22   MS. BAISH: It's on. Can you hear me? One

1 quick question on page seven you mentioned that you're

2 not there yet. Where -- tell us where you are right

3 now just in terms of your application goals.

4   MR. HANNAN: The chains of custody?

5   MS. BAISH: Right on page -- where you have

6 on page seven, you know, provide assurance that a

7 document, that the source identity is named, that GPO

8 is the source or OFR is the source, that it hasn't been

9 altered. And then of course the very sticky third rule

10 about chain of custody.

11   MR. HANNAN: Sure, so for PDFs today, those

12 first two absolutely are already provided. The third

13 one is easily providable, there is a little

14 coordination with content originators on the PDF

15 specifications, if you will, providing a place for

16 follow on signatures. We really haven't quite gone

17 there yet but we're fairly easily able to provide that

18 kind of thing, potentially working with content

19 providers in the Congress, for example, or the Federal

20 Register on that, for PDFs.

21   So for PDF the techniques line up pretty

22 well. And one of the subjects for today is some of the

1 choices regarding XML, dated XML or other formats that

2 people want to talk about.

3   MS. BAISH: Thanks.

4   MS. ZWAARD: John, can I jump in reason

5 quick. So a few things that FDsys does --

6   MR. HANNAN: Can you go ahead and state --

7 yeah.

8   MS. ZWAARD: Sorry.

9   MR. HANNAN: Your name, organization.

10   MS. ZWAARD: This is Kate Zwaard, and I'm

11 from GPO. So in order what FDsys is doing for

12 authentication, providing the identity of the publisher

13 for the document, we do do that in metadata. So if

14 you're a direct user of FDsys, if you're not receiving

15 that file from an intermediary, and you trust FDsys as

16 a repository, you can be assured that the document

17 you're looking at is provided by that issuing agency

18 from metadata we provide you.

19   In terms of providing assurance the document

20 wasn't altered since publication, we do provide

21 checksum (ph), a hash using the shop 256 (ph) algorithm

22 for each file we make publically accessible. So if

1 you're technologically able, you can check that

2 checksum to make sure it wasn't maliciously altered.

3   And in terms of chain of custody, we haven't

4 gotten as far as being able to make reliable that it

5 hasn't been altered, but we are using the premise data

6 dictionary and premise schema to provide a digital

7 (inaudible) chain of custody from the issuing agency

8 through all of the things we do to make sure that it's,

9 you know, we digitally sign it, we do checksums, we

10 identify the file format, so it gives you that long

11 list of things that have happened to the file since

12 we've received it.

13   One of the things GPO is also, you know,

14 thinking about is how does authenticity of a document

15 change over time once we're doing digital preservation

16 things to it. So once -- when we're migrating

17 documents to preserve it, you know, it may be altered a

18 little bit. How can we assure users that that's still

19 authentic, that it still contains, you know, the meat

20 of the content. And so that chain of custody allows

21 the user to inspect that and make that decision

22 themselves.

1   MR. HORTON: Could I just ask one question,

2   and I'm not sure if this apropos, but is there a sort

3   of intellectual premise here that material in a digital

4   format is unreliable? Or is the premise that it's just

5   de facto because it's in a digital format? Or is it

6   reliable until proven otherwise?

7   MR. HANNAN: I think that's an interesting

8   question. And so this is John Hannon from GPO. The

9   way I would address that is the fact that information's

10 in digital form provides more means for nefarious

11 actors and the ecosystem to be at work if they wanted

12 to. And therefore some additional thought processes

13 and techniques might be appropriate to help the

14 community assure itself when they are looking at a

15 digital data object of something. So yeah, that's how

16 I would look at it.

17   MR. SCHWEICKHART: Reynold Schweickhart from

18 GPO. I think particularly when you think about the

19 timeframe that GPO's responsible for providing

20 authenticated federal content, sort of life of the

21 Republic, over that span or even if you go back just

22 before Y2K, digital media is actually pretty fragile.

1 And so it's at this point more fragile than high

2 quality archival paper stored in many locations under

3 correct circumstances. I think that is the reason why

4 we're going to look more at how we do visual

5 authentication.

6   MR. HANNAN: Let's go to Mary Alice, because

7 I think you were ready and then we'll go to the back of

8 the room.

9   MS. BAISH: Because I never did get my

10 question, but just based on what you said, I mean the

11 whole issue of the cyber security is a really critical

12 one. And I know Senator Lieberman in fact just

13 introduced a bill on cyber security and DHS is probably

14 going to take the lead, but those are crucially

15 important when our government relies on so much

16 information that is only available an electronic forms.

17   Just my comment about your goals, you know,

18 are these enough. I think in an ideal world it would

19 be nice if every member of the public knew that they

20 could go to GPO Access and they will find the official

21 electronic version of the Federal Register or a law.

22 But I think the fact is with the growth of Google and

32

1 everything else people just go anywhere to look at the

2 information and make the assumption that it is perhaps

3 an official version and they can rely on it and they

4 can trust it and they can use it.

5   So I think one of the ultimate goals which I

6 would like to see if that whether I download a public

7 law from GPO Access or whether I come to FDsys and look

8 at it there or whether a court opinion is in --

9 available through a third party commercial publisher,

10 it would be very nice if at any -- under any of those

11 scenarios, wherever the electronic file resides, a user

12 could check the authentication if that's what they

13 needed to do.

14   MR. HANNAN: Right. I think would be great

15 for the whole system.

16   Lyle Green had a question. Can you give the

17 mic to Lyle? If somebody could pass the mic. Thank

18 you, Kate.

19   MR. GREEN: Lyle Green. Just wanted to bring

20 out one other -- I guess a different aspect on the

21 question about the reliability of digital format. The

22 authentication doesn't really bear on the issue of

1 whether the printed document matches the electronic

2 version. Authentication, you know, is more geared to

3 any alteration to the digital version. But as far as,

4 you know, we make the assumption that the digital

5 version matches the printed product but there is no

6 control in the process that verifies that.

7   MR. HANNAN: Well, you know, I mean Mike or

8 Reynold do you all want to comment on that? This is

9 John Hannan from GPO. You know, I think the -- Kate

10 kind of spoke to this too a little bit, about internal

11 processes at the GPO in terms of receiving information

12 electronically or otherwise from source agencies as

13 well as the topic that Lyle just brought up about

14 printed things that GPO obviously is control of

15 producing and the electronic version. So there are

16 some things there at GPO that help assure that those

17 things line up.

18   MR. SCHWEICKHART: This is Reynold

19 Schweickhart. I would just say that in the production

20 process there are quality assurance steps to assure the

21 electronic and paper product are synched up. I think

22 that's a general issue as we look at importing content,

34

1 for example, from websites where documents can be

2 posted. We don't have that same deep knowledge about

3 production process at that particular agency to be able

4 to ascertain whether that document, in electronic

5 companionable form in fact is identical or you've

6 gotten a slight revision somewhere along the line.

7   MR. HANNAN: That's a very good point. All

8 right, question over here.

9   MR. BENNETT: Hi, Daniel Bennett with the

10 eCitizen Foundation. One of the things that is going

11 on in the entire federal government is the data.gov and

12 other efforts to put out information and to have that

13 sort of swimming out there. And so the question of

14 authentication in terms of that form of data I think is

15 going to be solved not so much by encryptographic means

16 but by using URLs that can -- where you can find things

17 and be able to cite to them.

18   I mean people are grabbing things and so they

19 grab a portion of the census data, they grab a portion

20 of other things and they mash it up with what Mary

21   Alice was talking about a portion of

22 something that's published by the GPO, the question is

1 how -- when those things get mashed up can you

2 authenticate them. And having a good URL citation

3 system so that people can go back to the https:// and

4 having that embedded within all of the electronic

5 documents, when people grab pieces of it they'll be

6 able to do it. And then the other aspect of that, if

7 you think about it is, then we can externally hash

8 things and put -- and not just have GPO hash them but

9 other people will be able to grab portions of things

10 which will include both the reference back to the

11 authentic version that will be captured as it goes

12 through a long chain of custody, always pointing back.

13   And then also allowing more people to not

14 only have copies that can be referenced and just see

15 that they're all the same, but do their own hashes so

16 it isn't just the centralized hash that everybody has

17 to trust, but more and more people. I know as

18 specialists we think of this as a much more distributed

19 publishing system (inaudible) other government agencies

20 and commercial organizations putting out data

21 themselves. That's another way to think about it.

22   MR. MAYER: This is Jonathan Mayer from

1 Stanford. I guess going to the factors on page nine,

2 it seems to me that a serious concern as we think about

3 this would be what consumer is the data targeting, the

4 authentication practice we're targeting. So certainly

5 extensibility, standards and so on are very important,

6 but the extent to which they're important you could

7 imagine differing substantially based on the consumer.

8   So for example, if you're targeting your data

9 release to a web intermediary it might be -- well it's

10 important for it to, you know, carefully display in an

11 easy format the authentication mechanism, on the on the

12 other hand, not if you're targeting the casual

13 consumer, then you might want to think more about some

14 sort of commercial software that just displays the blue

15 ribbon and so on. And so as we go forward that seems

16 to me an important factor.

17   MR. HANNAN: Other questions? Yes.

18   MR. YU: This is Harlan from Princeton. I'm

19 wondering whether we should be thinking about data

20 that's coming out of agencies as well as data that's

21 coming out of the GPO. So, you know, once we start

22 distributing the authority to sign documents, say at

1 the Department of Labor, then there's a big key

2 management problem. And so I was wondering whether or

3 not that's in the scope of today's discussion or we're

4 just talking about documents that are coming out of GPO

5 where, you know, we have a private key and we can sign

6 things related to that, to deal with the key issue.

7   MR. HANNAN: Sure, Harlan.

8   MR. BOOTH: And I want to add on to that

9 actually.

10   MR. HANNAN: Yeah, sure.

11   MR. BOOTH: One of the things that I think --

12   MR. HANNAN: Could you go ahead and let

13 people know -- if you don't mind.

14   MR. BOOTH: Oh, Harold Booth. One of the

15 things that I wanted to add on to Harlan's comment is

16 that I think one of the things that you may want to

17 determine is that you have lots of signers and lots of

18 verifiers or do you have just a few signs with lots of

19 verifiers? It seems to me you have lots of verifiers,

20 so I think I've already got that answer. The real

21 question is do you have lots of signers? And I think

22 that kind of dovetails with Harlan's question.

1   MR. HANNAN: Yeah, and I think the chain of

2 custody topic really speaks to -- yeah, we do have a

3 lot of signers, potentially, if content originators,

4 you know, choose to do that. So I think that's the

5 challenge for the GPO obviously is to be able to, you

6 know, set up a -- or to look at providing and

7 facilitating things that may get extensible to either

8 case, the case where there are lots of signers and

9 obviously there are lots of verifiers.

10   MR. YU: Is it the role of the GPO to provide

11 a signing service for the rest of the agencies? Is

12 that something that's in the scope of what the GPO

13 might do or --

14   MR. SCHWEICKHART: Let me --

15   MR. HANNAN: Yeah, go for it.

16   MR. SCHWEICKHART: My short answer is if we

17 could make money at we would. Just a couple of

18 comments. Our PKI is cross certified with the federal

19 bridge. So from a chain of custody point of view we

20 could certainly pick in documents that when signed by

21 any federal employee, contractor, anyone who's a

22 participant in that bridge process, one of the things

1 that we think about in that context, however, is the

2 re-authentication problem of what do you do 100 years

3 later in terms of looking at that chain of custody.

4 Where -- how do you sort of nail down that

5 authentication as sort of documents enter the system,

6 as they become part of the FDsys and so on.

7   And so I think there's two parts for that,

8 but broadly speaking we're set up to take -- and in

9 fact when we took the first federal budget from the

10 White House, it was signed by a White House employee

11 with a digital certificate on their HSPD-12 card to do

12 that. So we have a -- I think we have a robust

13 infrastructure depending on where we go from a policy

14 direction.

15   MR. BOOTH: I'd like to ask a question

16 regarding that particular point. How do you know who's

17 the authoritative person for determining that that was

18 the budget? So let's make it more general, for a

19 particular document how do you know that that's the

20 person that's responsible for doing it, as opposed to

21 maybe having -- as an individual how would I know that

22 if there was some ort of general purpose White House

40

1 budget certificate that then would be kind of clearly

2 labeled, that's the role that that certificate is

3 intended to play.

4   MR. HANNAN: Well let's --

5   MR. SCHWEICKHART: Yeah, I was going to --

6 let me answer that shortly and then maybe if we get

7 more technical we may want to take it offline and go to

8 other topics. But that's really an out of band (ph)

9 process today. We know who the person at the White

10 House is, the Federal Register knows who at the

11 Department of Labor is authorized to issue regulations

12 and so there's a out of band process.

13   MR. HANNAN: In today's world, and there are

14 ways of moving that into an electronic world with

15 education, some communication about that. These are

16 challenges that we've always had in the tangible world

17 and solved them quite easily and I think we'll be able

18 to do that, although it will take come some

19 communication and there will be a change in process for

20 people. Jonathan (inaudible) for a second.

21   MR. DAVIS: Rick Davis, Government Printing

22 Office. Adding to that point, from an agency

41

1 perspective, at GPO on the XR519 certificate it's

2 authorized by the Superintendent of Documents which is

3 me. In terms of our policy that we have written, in

4 terms of other federal agencies, we actually ask that

5 it be at the head of the agency level or a designated

6 authority by the head of the agency so it's coming down

7 from the top down.

8   MR. ANDERSON: Steve Anderson for the

9 Maryland State Law Library. I'd like to reiterate what

10 Reynold said about making sure that the chain of

11 custody in effect and the authentication principles are

12 in effect for the life of the Republic. I think

13 looking at the long term and the longest tail we can on

14 these documents is going to be very important. Coming

15 from a private law firm background to the State Law

16 Library several years ago and finding that we had 400

17 year old books on the shelf was an eye-opener. And I

18 want to make sure that -- it would be nice to make sure

19 that whatever we do is going to last, you know, as much

20 as possible.

21   Going along with that, I don't mean to

22 suggest that we do take any type of blocks approach in

42

1 terms of having duplicate copies of an authenticated

2 document because that just gets weird. However, I

3 think being able to have some type of very quick, easy,

4 on the fly redundancy measure and enabled to pour

5 things over between system and system is very

6 important.

7   MR. HANNAN: Thank you.

8   MR. BENNETT: I think that --

9   MR. HANNAN: Can you just for the

10 transcriber's benefit, restate your name.

11   MR. BENNETT: Sure. Daniel Bennett with the

12 eCitizen Foundation. I think having drafted the first

13 legislation on e-signatures, electronic signatures, I

14 think we're having a little bit of potential confusion

15 but I think we might as well just talk about it, in

16 terms of authentication because they're signing

17 something so a lot of stuff which is legislative,

18 people co-sponsor, it gets signed by the President,

19 there's authentication for the purpose of just signing,

20 which is separate than the authentication for the

21 purposes of things like identity for the purpose of the

22 chain of custody to know who was there. But it is a

1 weird thing once you move into electronic and you have

2 people's -- what look like physical signatures and

3 representations in the future perhaps of their

4 electronic signature, that you will get into a bind of

5 how you deal with signatures in that sense for

6 authentication versus authentication of making sure the

7 document itself is authentic.

8   So it's something -- we might as well start

9 understanding and thinking about it. But for now

10 probably just want to put that to the side and just

11 understand that we're talking authentic documents and

12 chain of custody issues and not the other.

13   MR. YU: And if I could just add to that

14 really quick. I also want to make sure we're clear on,

15 in terms of terminology when we talk about

16 authentication I think that that basically guarantees,

17 you know, who that document came from. There's another

18 topic or another concept of integrity which is what

19 hash functions give you. Right? So when you use a

20 hash on any pile of bytes all that gets you is

21 integrity, it doesn't give you authentication. It

22 doesn't tell you who hashed that document, who made

1 that document, but a cryptographic digital signature

2 would give you both.

3   So I was concerned in the earlier slide when

4 you talked about less robust means, I was worried that

5 if you use something that was less robust like a hash

6 that didn't involve any (inaudible) material, then you

7 would only get integrity and you wouldn't get

8 authentication.

9   MR. HANNAN: That's exactly right. We have

10 some slides to try to get that very point to kind of

11 comparatively analyze some of the techniques out there.

12   So this has been information that at GPO

13 we're pretty familiar with. You know, and it kind of -

14 - Harold's question really sparked that thought, which

15 is good, about there are many ways to electronically

16 sign a piece of information. The Electronic Signature

17 Act, it's technology neutral, it gives lots of

18 different options for how you can do that. And so that

19 is different from the electronic authentication of a

20 document, although interestingly enough you can kind of

21 use some of the same concepts in both arenas. So we'll

22 talk through more of that today, a little bit. I think

1 that's a great comment.

2   MR. GALLUCCHIO: Hi, this is Tim Gallucchio

3 from the Department of Defense. I just wanted to warn

4 you that adding a long tail on this document signature

5 is a worthy goal and should be done to the fullest that

6 you can. But you should also -- you should also

7 realize that this is, you know, you will have to resign

8 eventually, whether the (inaudible) gets broken or just

9 when time expires. Computing is getting better all the

10 time, faster and faster, newer craze so eventually the

11 (inaudible) is going to expire and you will have to

12 resign and maybe we'll all be back here or our children

13 will be back here at a similar workshop discussing

14 similar things.

15   MR. HANNAN: We do have a topic later talking

16 a little bit about that thought process of re-

17 authentication over time, not so much to get a lot of

18 input, because -- although we're happy to -- again,

19 it's more just to a brief on what we're doing. Great

20 comment, yeah we're aware of that. Some techniques can

21 be more involved in that regard than others.

22   MR. GALLUCCHIO: And I also -- I don't know,

1 the way I see this, I take it you would provide a

2 method that supports authentic chain of custody. I

3 think you want to propose this standard, you know,

4 you're providing a standard and then you're going to

5 have different companies implement this standard and

6 then the user will go to this webpage and then they'll

7 click on it or --

8   MR. HANNAN: Well, I think that's interesting

9 because we're not really a standards body, you know, so

10 that really is why it's stated that way. I appreciate

11 your comment, but we're really not in the business of

12 creating international open standards for everyone on

13 the planet. That's why we've got a lot of folks here

14 from different constituencies so -- again I think GPO

15 is ready to take advantage of the best thinking and

16 possibilities that are there to help bring value to the

17 community. And this workshop is an example of trying

18 to get some of those. Thanks.

19   MS. BAISH: Very quickly I wanted to comment

20 on your point, John. Mary Alice Baish, American

21 Association of Law Libraries.

22   Going back to your point is that blue ribbon

47

1 on top enough for most people? Yes, the answer is

2 probably yes. What GPO has done in terms of your

3 progress on digital authentication is based on what

4 France did enacting a law in 2004, making their

5 official Gazette the electronic version, authenticated,

6 secure and capable of using in a courtroom as the

7 official version. And what France does is actually it

8 has two separate databases for its official Gazette.

9 One is a very user friendly Google-type database and

10 anybody can go and look for information and find it.

11 And they're just looking at -- for information only,

12 they don't need to have that authenticated chain of

13 custody to print off and to take along with the

14 printout of the regulation or the order into the court.

15   So I think given the fact that you have made

16 progress on your public and private laws and the

17 congressional bills, certainly from our perspective we

18 would like to see you keep up that work, and your top

19 priorities obviously being the electronic legal

20 information. And I'm sorry that nobody is here

21 representing the federal courts, but I'm sure you're

22 having discussions with them, hopefully on this very

1 topic. Thank you.

2   MR. HANNAN: Thanks very much. Just one

3 quick comment and then we'll move on, because I think

4 this has been great input and that's what we expected

5 was a lot of different viewpoints based on the

6 diversity of the stakeholders. Is that the comment

7 that Jonathan made earlier is something we are aware of

8 and thinking about is that the needs of the individual

9 user citizen and the needs of large automated

10 intermediary processors information, those can be quite

11 a bit different. So we're trying to think about what's

12 the best achievable, practical way that we can try to

13 help the community in that regard.

14   With that, if everybody's comfortable, let's

15 move to the next slide. Thanks, that was a lot of

16 really good input. And so that is this slide which is

17 number ten in your handout set. And it's thinking

18 beyond what we've been doing. And we've already talked

19 a little bit about this, you know, information beyond

20 information captured in PDF files.

21   The digital signature approach has been

22 fairly effective, again for at least some parties in

1 the ecosystem. You know, in that regard it kind of

2 seems like it may be something to think about in the

3 next types of data or such, so that was just one

4 observation from our point of view.

5   A question is, you know, is a second

6 assurance level technique like hash based schemes, that

7 may not do as Harlan alluded to, as much as

8 cryptographic digital signature techniques, are those

9 still valuable and should that be another channel that

10 we think about offering or supporting or facilitating

11 somehow for the community. Kind of a complicated

12 question actually and there are a lot of different

13 facets to it. We have a slide that kind of compares

14 some things on the next table. What you get, what do

15 you not get? What do techniques tend to naturally

16 support without a lot of other application business

17 rule processing which might vary from person to person

18 or organization to organization? What techniques kind

19 of lend themselves to certain capabilities that we

20 talked about before?

21   So let's go to that table on the next slide

22 real quick and then talk through that just a second,

50

1 then we'll come back to what do people think about that

2 question of hash based techniques and such.

3   So this table is, you know, pretty

4 simplistic. So please, there -- we tried to make this

5 something that would be -- something we could at least

6 talk to for today but we basically -- on the far left,

7 the methods we basically, hash based methods using HSA

8 or SHAW-256 (ph) and other kinds of techniques, which

9 provide a digital thumbprint of a particular set of

10 digital bytes. And then there are the digital

11 signature techniques that, you know, we use today in

12 the PDF world.

13   So across the top row there are some

14 different factors that seem to be important or

15 interesting for our decision making as we try to decide

16 how best to support the community in this regard. So

17 the first one was there's a trusted third party

18 involved somehow and with hash methods, you know, at

19 the end of the day there has to be some other parties

20 involved for trust. Is it only one or multiple third

21 parties? Well at the end of the day there's some other

22 third party involved. You know, could the third party

1 be GPO? Well, you can -- for hash based schemes it

2 seems like it could probably invent one if we wanted

3 to. I'm not saying whether that's good or bad, there

4 are probably thoughts on both sides of that equation.

5   The next column is does it use open

6 standards? Again, facilitate the ability of many

7 parties to innovate around it (inaudible) proprietary,

8 obviously that slows innovation (inaudible). Yes, for

9 hashes and yes for digital signatures. So on the first

10 -- those first three areas it seemed like they're

11 pretty much each other technique and, you know, has

12 these features to them.

13   That fourth column is does the method show

14 the publisher, disseminator of the document --

15 publisher might not be the exact right term, so forgive

16 me, I'm more on the technology side, that may be a

17 loaded term. But to Harlan's point, hashed based

18 methods themselves don't do that alone, there has to be

19 other business processing rules, information to do

20 that. Does the digital signature provide that

21 capability? It easily can be used for that so it kind

22 of in and of itself provides you a ready-made way of

1   doing that. So that seemed to be one where the methods

2   kind of were different.

3   The next one about facilitating a chain of

4   trust, it seemed to us that hash based methods, you

5   know, just by themselves really did, for the same

6   reason they don't really support who the source is,

7   they really don't support, you know, obviously going

8   back further into the supply chain of a digital object,

9   you know, who's been handling it or where did it come

10 from along the way. It's not to say it couldn't, but

11 in and of itself it really doesn't. It has to have a

12 lot of other coding and techniques and business process

13 rules on top of it.

14   Digital signatures on the other hand seem to

15 have kind of a ready-made way of providing a way to

16 quickly get a sense of that. Not to say that there --

17 you know, there have to be some understood business

18 rules around the concept of the signature is in this

19 place, that means, you know, first party with the

20 document, here is the second party. There would have

21 to be some rules of engagement. And we talked about

22 that a little bit earlier about, you know, how do we

1 really know, in a tangible world, who the source of a

2 file was that gets bound into a book. I mean there's -

3 - you know, there would have to be some business rules

4 around any process.

5   So again, the digital signature seemed to be

6 a little bit more ready-made, not that it's perfect but

7 any means, or solves all the problems. Hashes, not

8 that it couldn't do it, but didn't -- you know, kind of

9 baked in didn't have as much ready-made for that. So a

10 little bit of a difference there.

11   Free client software available for users,

12 again this is the citizen user. Yeah, it seems like

13 that's pretty easy on both counts. Is this method

14 included in the (inaudible) guidance for electronic

15 authentication? You know, digital signatures, yes.

16 Hash based methods, no. Now that particular

17 publication is really oriented a little bit more to

18 who's the source of something. It's that topic you

19 mentioned earlier, Daniel, about you know, the subtle

20 difference between did I sign, and my signatures on

21 this document versus it's the official one that got

22 bound into a book.

1   So to be fair, in this publication please

2 Harold jump in and add things if you want to, but that

3 publication is focused on authentication of the source

4 of material, so that's why digital signatures do lend

5 themselves to hash-based, not really mentioned in that

6 particular publication. But those are one of the

7 things that we look at, the GPO tries to take advantage

8 of all the good standards work that comes out of this

9 other agency (inaudible). And we'll talk about that a

10 little bit later for XML too. Lots of other standards

11 bodies, you know (inaudible) standards bodies across

12 the international and the national space.

13   Is offline validation possible? It can be

14 possible, in the second row there, with cryptographic

15 digital signatures if one's clever about it. It's

16 really not possible, we don't think, with hash-based

17 methods. Now is that important? Well maybe it is, you

18 know, maybe it isn't. If somebody's on an airplane, is

19 it a big deal? Can they wait till they get down and

20 maybe in an airplane that -- being on the Internet

21 would be easy too. There are probably some other

22 scenarios where is this helpful or you know, not.

55

1   So anyway, we thought that was kind of an

2   interesting, to us these were some important factors

3   and ways to kind of compare and contrast. So with that

4   I think we'll just kind of open it up there. I'm sure

5   there are lots of other factors and ways to think

6   about, so that's really the purpose of today was to get

7   some input from folks so that we're not just in an echo

8   chamber here at GPO writing these.

9   I think, did you have a comment Jonathan?

10   MR. MAYER: I just had a clarifying question.

11   MR. HANNAN: Okay, sure. We'll go there and

12   then we'll go to Harlan, I think Harlan you had one.

13   MR. MAYER: So when you're talking offline

14   and validation --

15   MR. SPEAKER: Can you announce who you are as

16   well, please.

17   MR. MAYER: This is Jonathan Mayer from

18   Stanford. A clarifying question on offline validation.

19   So are you mentioning here (inaudible) some sort of

20   authentication on top of let's say HDTPS (ph)? Is that

21   the idea? I'm not following how offline validation of

22   a hash itself is not possible.

1   MR. HANNAN: Well I think -- that's a good

2 point too. The concept would be that you have a way to

3 offline valid the content itself. Now if you pre-

4 stored all of that, which is essentially what happens

5 in the techniques for cryptographic digital signature,

6 at the time of signing a lot of information is put

7 together to make it easy to validate without having to

8 be connected to the Internet or any network. Yeah, you

9 probably could do that with hashes if you did all of

10 that ahead of time, for the purpose of saying, is that

11 document the document that was on the URL, you know,

12 two months ago. So I don't know if that answered your

13 question. It looked like it didn't, but --

14   MR. MAYER: I guess I may be recalling --

15 mis- recalling my computer security class from

16 undergrad. But some cryptographic digital signature

17 techniques rely on taking a hash and then sign it.

18   MR. HANNAN: Almost every cryptographic

19 digital signature technique does.

20   MR. MAYER: Right. So that's why --

21   MR. HANNAN: It builds upon that.

22   MR. MAYER: Right. So the same validation

1 technique you would need to check a hash is -- or I

2 should say, the technique you need to check a hash is a

3 subset of what you need to check a digital signature.

4   MR. HANNAN: Well, this kind of goes back to

5 the concept of really knowing the source of the

6 document, not -- you know, that's what we mean by

7 validation is knowing both that the document wasn't

8 altered but that you know the source of it. So that's

9 really -- inherent in validation is the concept that

10 you know the source. And with hash-based techniques

11 you just -- you don't know the source. That's why it's

12 a building block, of course of cryptographic digital

13 signature techniques. It doesn't have to be, but for

14 efficiencies purposes it almost always is (inaudible).

15 That's just really for computational efficiency

16 (inaudible).

17   MR. BOOTH: You may want to use the term

18 "verification" instead.

19   MR. HANNAN: Okay.

20   MR. BOOTH: That's the more common used term.

21   MR. HANNAN: Okay. That's good. Okay.

22 Yeah, no that's -- I think that's one of the

1 challenges. There really isn't a lot of -- you know,

2 the standard terminology is tricky sometimes even for

3 somebody in my space. So but that's great, we'll use

4 that from now on. That's good. Thank you. And Harold

5 -- I mean Harlan, I think you had one.

6   MR. YU: I had the exact same question as

7 Jon. It seems like if cryptographic signature on the

8 right hand column is yes then that should also be yes

9 or an N/A if that's the wrong question to ask.

10   MR. HANNAN: We'll try to clarify that. And

11 that's what the purpose of today was to get some input

12 and not trying to say this is the be all and end all,

13 but that's really good. That was the differentiating

14 factor was the source of the (inaudible).

15   MR. SHULER: John Shuler, University of

16 Illinois in Chicago. I want to ask it from another

17 direction. How many users of GPO Access or potentially

18 FDsys actually expect this level of authentication or

19 verification from the stuff they draw down from your

20 website?

21   MR. HANNAN: That's a great question. I think

22 (inaudible).

59

1   (Multiple comments.)

2   MR. DAVIS: Rick Davis, GPO. I think when we

3   began the authentication effort it was primarily at the

4   request of the library community, particularly AALL.

5   What's been interesting is I monitor our customer

6   relationship management software on a daily basis to

7   sort of get the pulse of the American citizen when

8   they're coming in with questions. I don't think we

9   would have gotten questions five years ago about

10   whether or not this document is authentic, they just

11   want the information. What we're finding now is not

12   only from librarians, not only from researchers, not

13   only from historians but citizens, people writing

14   essays as 16 year olds, we're getting questions about

15   what source should I cite as official. And I think

16   it's an ongoing educational process to realize that

17   when you're looking for something the first result

18   that comes up in a search engine like Google is not

19   necessarily your source that you want to put in your

20   research paper.

21   So I think there was an early learning curve.

22   I think it's getting better but I don't think it's --

1 you know, 40 million users of GPO Access but I think

2 it's growing and I think where it is five years from

3 now is going to be different from where it is today.

4   MR. SHULER: But isn't there a difference

5 between being official and being authenticated or being

6 verified?

7   MR. DAVIS: There is an -- several

8 definitions of that term. I won't go into deep detail

9 on this with the audience, but authentic from the

10 standpoint that we want to ensure that the information

11 is unchanged from the time it left the Government

12 Printing Office, official from the standpoint of we

13 have, I mentioned early on in my remarks that a lot of

14 this content is born digital now with no print

15 equivalent. And in some cases, like with the Office of

16 the Federal Register, they're recognizing that the

17 online content made available through GPO Access and

18 now FDsys is the official publication.

19   I think we're going to be seeing more and

20 more of this, particularly where you have no print

21 equivalent.

22   MR. BENNETT: One thing that may sound

61

1 strange that isn't in the line is the idea of authentic

2 meaning that you can find it at an official place. And

3 so for example, you have a paper copy of something, you

4 know, to print something out and you give it to someone

5 then you -- digital stuff, the digital certificates and

6 signatures don't show up, all you get is the ribbon or

7 whatever. So I think one of the interesting aspects of

8 authentication is a unique identifier, specifically a

9 URL, that should be printed with everything and that

10 way anyone who gets it -- the printed thing, so you can

11 help authenticate the paper that way.

12   But the other aspect of this where you can

13 start thinking about providing authentication not from

14 encryptographic means, but through unique identifiers

15 is a document can have multiple sections. You're going

16 to get into a law of diminishing returns if you try and

17 sign each portion of it. But if you have a unique

18 identifier for each portion of it, say a ID attribute

19 so it could have a fragment URL which becomes a unique

20 identifier, as you do that for your documents and that

21 they're human readable, then what you have is a method

22 again of if people do want to have hashes or digital

1 signatures, they can add that externally, they can do

2 hash trees so that they can, instead of having one

3 document, quote "be authentic," you can have groups of

4 documents be authentic because you've done an external

5 hash that has all that information. And it could be

6 portions of the document that you are authenticating

7 for some purposes and not the entire document.

8   This is another way to I think draw out what

9 authentication could mean. And the other aspect of it

10 to think about is if you have a URL that points to

11 something and you can go look for it, but it's really

12 also used as a unique identifier, you could have, in

13 your closet, you could warehouse a physical object that

14 has that same unique identifier and you could always

15 take the electronic one over to it and you know, have

16 that citation or a URL and look at the two things.

17   So again, I think having unique identifiers

18 is a real key to this because you can create fake bills

19 that don't exist. How do you know a fake bill doesn't

20 exist? Well you know, with this signature on it, how

21 do you know who's signature is it? It's a long

22 process, but the more you can think about things as

1 repositories and authenticating (inaudible).

2   repositories from using unique identifiers I

3 think might be helpful as an added authentication.

4   MR. HANNAN: Yeah, it gets very challenging

5 when you start thinking about tangible paper documents

6 (inaudible). Yes?

7   MR. ANDERSON: Steve Anderson. One of the

8 things that intrigues me about offline validation and

9 maybe that can be encompassed within your comments I

10 suppose, but is considering what the life cycle is, at

11 least in the near term, of a particular document. And

12 one of the things that these state courts are working

13 on, I'm not necessarily going to speak for PACER or

14 anything else like that, but one of the things that I

15 think the judiciary envisions, at least in the next 10

16 or 15 years is significant e-filing.

17   One of the things that would go along with

18 that would be the ability to capture something from the

19 U.S. Code, Congressional Record, Federal Register,

20 etcetera. Have that be authenticated for the life

21 cycle of the use of that as an attachment in a case, so

22 that if you are putting that in as part of a memo or a

1 pleading or a brief or something of that nature, you

2 not only have your parties, you know, official thing

3 being submitted to whatever court system there is, but

4 you are going to be attaching your relevant case

5 document from GPO or, you know, whatever else exists at

6 the time.

7   You want to make sure that that is going to

8 be authenticatable through the life cycle of that

9 offline and online usage during the e-filing process.

10 So when a judge gets it, you know, on the -- when he's

11 finally taking a look at that file, the case file, that

12 there's something that's going to be authenticated on

13 his computer or her computer. And there are probably

14 other significant uses like that in terms of academia,

15 making sure that you can attach, as an appendix to some

16 type of online publication, whatever report from

17 whatever federal agency there is. So the offline

18 possibility needs to be taken into consideration that

19 there are going to be lots of, you know, attachings and

20 detachings throughout the usage of that particular

21 document, in my view. Thanks.

22   MR. GEE: Robert Gee, from the Law Library of

65

1 Congress. I wanted to note -- excuse me, can you hear

2 me? To dovetail on what Steve was just saying, the

3 authentication issue right now is that there's actually

4 statutory provisions that would have to be amended as

5 it relates to what is considered the legal evidence of

6 the laws of the United States. Right now we have three

7 separate publications that Congress has designated as

8 the official text of the laws for the courts to -- or

9 that constitute the legal evidence of the text of the

10 law of the United States. And one relates to the

11 statutes at large as being the printed version, the

12 other is the United States Code as the (inaudible) law

13 and through the United States Code, and then the

14 treaties. And those three publications right now have

15 only print as being the official source and therefore

16 that is the authentic, official version that can be

17 introduced.

18   So I think that as -- and I think the courts

19 - - I shouldn't speak for them, but I would suggest

20 that they would be very interested in seeing something

21 that can be completely reliable in a digital format

22 before they are going to be allowing those types of --

66

1 those particular publications to be introduced as

2 evidence of what is the law of the land.

3   MR. HANNAN: Very, very good point. If we

4 get in the GPO help what we do to further that, then I

5 think it's kind of a win/win (inaudible).

6   MR. HORTON: Bob Horton from the Minnesota

7 Historical Society. Could I ask if we could add one

8 factor to this, as basically any implication for long

9 term preservation? Just talking from someone who's a

10 state archivist I mean what I could sort of guarantee

11 of the state level possibly (inaudible) level as well,

12 that anything that produces a barrier for long term

13 preservation is problematic, extremely problematic. So

14 you may want to separate the functions that

15 authentication may have some short term need as opposed

16 to some long term function, either the -- anything that

17 you do for an authentication rationale may have --

18 become an impediment for long term preservation and

19 authentication down the line.

20   MR. HANNAN: Well I think that's a great

21 comment, thank you. It's analogous to, in the same

22 spirit as the comment made earlier about citizen use

1 versus high speed, high volume automated. Those are,

2 you know, preservation versus, you know, immediate

3 verification, those are part of the different use cases

4 or (inaudible) so they -- yeah, that's the art or the

5 trick, right, is to find, hopefully, something that

6 will help on all fronts or have a small number of

7 things that get brought to bear. Boy, that's a great

8 comment.

9   MR. HORTON: Plus it argues also for I think

10 maybe the larger context or larger intellectual

11 framework because there's no kind of one solution to

12 this. There is one size fits all is just an impossible

13 dream. So maybe, you know, a different approach for

14 different constituencies, for different functions and

15 over time as well and among different organizations. I

16 mean I think there's a considerable difference between

17 the federal and the state level, for example, the state

18 level in terms of virtually all the functions we're

19 talking about, is a much more decentralized and much

20 more distributed set of responsibilities.

21   MR. HANNAN: Great. No, that's good. And we

22 -- or that's one of the real purposes of today is to

1 really start to get at some of the thought processes,

2 you know, like the question of is a second hash-based

3 method something we should be (inaudible). So other

4 questions, comments? I think at this point it's --

5   (Multiple comments.)

6   MS. DALECKY: Yeah, Selene Dalecky, GPO. I

7 just wanted to add a follow up question on the approach

8 that Daniel was talking about earlier. In terms of

9 tying the unique identifier into the URL, is there a

10 question of sustainability there with the transient

11 nature of URLs? And how is that accomplished from a

12 long term perspective?

13   MR. BENNETT: I think that that gets to a big

14 issue which is content management systems and producing

15 things with URLs. But one of the things that, you

16 know, Europe is dealing with is, you know, how do we

17 deal with this and have -- we're looking at URNs

18 because they're more abstract, etcetera. But I really

19 think that URLs are unique identifiers that have the

20 special, it's like photons, they both are waves and

21 particles at the same time, URLs are both unique

22 identifiers and location references. And so you have

1 to understand that they have those two capabilities.

2 And what we want is to recognize that over time they'll

3 still be a unique identifier. If something changes you

4 can still find them, say in other things, those

5 references. So you can use it as a metadata then you

6 can still find it.

7   So if you, as the federal government, decided

8 that you would create a URL that was, for a bill for

9 example, I think that's the easiest way to (inaudible)

10 example, you know, 111th Congress, HR1, right? And you

11 created a URL that contained that, can you ever imagine

12 creating -- using that URL for anything else? And so

13 the question is do you ever do it.

14   And in the future can -- aren't we at the

15 point where if we have other things we can always use

16 redirects or point to the older version or, you know,

17 use a way back machine, getting it archived so even if

18 the website goes down someone else will then be able to

19 use that unique identifier to find it and you know,

20 they are taking slices of the web at certain times. And

21 so there are different ways to get at it but I think

22 that it does mean that to avoid those types of

1 complications an organization, I think for the long

2 term should really think about how they structure the

3 URLs to try and make them as technology neutral as they

4 can.

5   MR. HANNAN: Other questions? Yes, Harold.

6   MR. BOOTH: Yes, Harold Booth. I don't know

7 if here in your space you have this need but if you

8 have URLs you have the necessity of having confidential

9 proprietary information within your space. URLs might

10 be problematic in that thing, because you may not have

11 things that are publically available to everybody in

12 order to do the verification or validation process. So

13 just to keep that in mind, I don't know if that's a

14 problem in your space, but just to put that out there.

15   MR. HANNAN: No, thanks I think that's the

16 purpose of today's workshop is to have a dialogue. The

17 concept of using URLs, you know, as the unique

18 identifier, interesting idea that we can see has some

19 things to be worked out as well. But it is

20 (inaudible).

21   MR. MAYER: I just wanted to add on this

22 question of secondary techniques, something to kind of

1 keep in the back of the mind and we can discuss further

2 as we go along. The threat model is particularly

3 important here. If we're concerned about errors in

4 transmission and storage and so on, hashes look a lot

5 better (inaudible). But as we start to move maybe

6 towards like the malicious klutz or towards the just

7 purely malicious actor then of course we need

8 signatures. So depending on the users needs and

9 depending on kind of the application, you could imagine

10 wanting the hash-based to protect against certain

11 things or signature protect against more things.

12   MR. HANNAN: That's a great way of thinking

13 about it. It looks like we're kind of at the point

14 where we probably want to take a break at this point is

15 what I was thinking. So if we can, it's about 10:35.

16 Why don't we convene at 10:50. That will give us a 15

17 minute break. And then we'll keep going.

18   MR. BRIEBE: The clocks about five minutes

19 off, so it's closer to 22 right now.

20   MR. HANNAN: Okay.

21   MR. BRIEBE: Just to be aware of it, if we're

22 going to take 15 minutes.

1   MR. HANNAN: All right, I thought my watch

2 was fast, but it's slow.

3   Okay, why don't we come back at five till.

4 Thank you.

5   (Off record.)

6   MR. HANNAN: Okay, everybody we're going to

7 start back up. We took a little bit longer break,

8 hoping that that was useful.

9   I think at this point what we'd like to do is

10 turn it over to Selene Dalecky of GPO to kind of lead

11 us into the next discussion topic, trying to synthesize

12 a little bit what we all discussed last hour or so and

13 how it relates to two forms of authentication for PDF

14 documents and whether that's something that communities

15 need or just want. So Selene, do you want to start

16 that out?

17   MS. DALECKY: This is Selene Dalecky from

18 GPO. I just -- there was a lot of good discussion early

19 on on techniques and when and how to apply them, in

20 terms of the electronic content. And I think some of

21 the things that came out that we would like to explore

22 a little bit more are, you know, the technologies

1 (inaudible) but also when would be the right time to

2 use them and what the needs are in terms of the use

3 cases for this content that we see, at least from the

4 GPO side.

5   And the two cases that we're looking at is

6 direct to the end user. So there is a person who is

7 looking for bill or looking for a law and needs to know

8 that that is the authentic version, the official

9 version, something that they can rely upon either in

10 their research or actually in a court of law. The

11 other would be data that's used for -- that's

12 repurposed for other means, so system to system where

13 we have, you know, a scraping or a bulk download from

14 data.gov or from our bulk directory of XML or other

15 content to be used either in total or to be mashed up

16 with other content. What are the needs there in terms

17 of conveying authenticity, conveying integrity to keep

18 that integrity and authenticity chain going past the

19 system to system delivery.

20   I think that another good area to think about

21 in this part is I think this is direct to the end user

22 but the use case that Mary Alice brought up in France,

1 where there's a system that's for information only

2 that's more usable, user friendly, searchable,

3 accessible. But then you always have the link back to

4 the official version that can be used appropriately in

5 serious research or in, you know, a court of law.

6   In other similar cases what we are doing with

7 a project called the FR 2.0, it's being done in

8 conjunction with the Office of the Federal Register and

9 where we are taking the XML content that's been

10 converted here at GPO from the SGML (ph) that's used to

11 print the Federal Register and using that to power a

12 search and a Web 2.0 interface to the Federal Register

13 to make it more user friendly to draw out and spotlight

14 the content that's pretty dense within a printed

15 publication itself or within the PDF version of the

16 printed publication.

17   But whenever you see the FR 2.0 results in a

18 section or an article that's presented, you will have a

19 link back to the signed PDF version since that has been

20 deemed the official version of the Federal Register, by

21 the UFR and NARA.

22   So we look at these different use cases.

75

1 Who's going to be using the content and for what

2 purpose is this content going to be used? Then the

3 question becomes what are the authentication needs for

4 those -- for that content and for that user? How does

5 it differ and is this something that we can decide upon

6 or that we can kind of put a path forward on and

7 develop needs around so that we can look at the

8 technological solutions to these approaches.

9   And John, I didn't know if you had anything

10 to add or if anybody kind of had some initial thoughts

11 on this and you could start the discussion around

12 getting use cases of who is getting the content and for

13 what purposes and how does that drive the

14 authentication and integrity needs to -- that

15 information on the integrity and authentication that

16 needs to be disseminated to the end user of this

17 particular content.

18   MR. HANNAN: Thanks, Selene. I think that

19 frames it pretty well. Let me just try to add one

20 thing to help spark some dialogue and that is we've got

21 -- already talked about, I think it's a very useful

22 viewpoint, of single individual user versus automated

1 system to system processing. So that's one way to

2 think about to breaking down the user/consumer cases.

3 Probably the first way to do it.

4   I guess the question is for automated

5 processes are there hurdles in the current

6 authentication models with PDF that prevent -- present

7 hurdles and problems? And if there are what are they?

8 And then is there something in the automated system to

9 system taking information from GPO processing it and

10 making it useful to other parties, is there something

11 in the current techniques that need to be improved upon

12 as we go forward?

13   MS. DALECKY: And I had one other thing to

14 add, as just kind of a nuance to the second case study

15 of the system A to system B content transfer as opposed

16 to the system A to end user content transfer. There's

17 the system A to system B content transfer and then

18 system B to end user. And the question there is,

19 assuming that GPO would be system A in this case, what

20 is GPO's responsibility to the end user who's using a

21 system in between the originating system and the user

22 of that content?

1   So again this would come in in case of

2   mashups or in the case of pulling out content from, you

3   know, a data set that GPO puts up on data.gov and

4   repurposing it and presenting it out to users in a

5   different format.

6   MR. HANNAN: So are there thoughts there or

7   burning desires to help guide us at GPO in this regard?

8   Or if not we'll just move on and go to the next one.

9   MR. SHULER: John Shuler, University of

10   Illinois at Chicago. If I understand your remarks, I

11   mean are you saying that GPO has an ongoing custodial

12   responsibility for stuff that originates from your

13   boxes, no matter where it goes and who uses it?

14   MS. DALECKY: That's one of the questions

15   that I'm posing to get feedback on.

16   MR. SHULER: How does that exist within GPO's

17   traditions of not having any copyright material that

18   they produce and distribute?

19   MR. HANNAN: Mike, do you want to take that

20   or do you want me to take it? Let me go ahead and give

21   you my own personal view of things as we're -- I mean

22   we're on the technology side, unless Rick or Selene,

78

1 you guys want to jump in.

2   MR. DAVIS: Feel free.

3   MR. HANNAN: I think the GPO approach is how

4 can we facilitate the authentic use of information that

5 we disseminate for the community and not provide

6 negative consequences to that. So I think what we're

7 really asking for -- and again, it's kind of abstract

8 in some ways, and this is I'm sure the first of a few

9 discussions potentially about this. But how can we,

10 through the use of -- and through making good decisions

11 about how to use some of the technical tools available,

12 how can we facilitate authentic content being assumed

13 downstream by other actors in the system.

14   MR. WASH: But let's dive into the data.gov

15 example, because it's a good one (inaudible) and to

16 your question, John, about the custodial or the

17 stewardship responsibility. You know, we have the

18 Federal Register and unfortunately Mike White from the

19 Federal Register couldn't make it today, but we have

20 the Federal Register content in FDsys and it's

21 digitally signed. And they have deemed that to be the

22 authentic and official electronic version of the

1 Federal Register.

2   MS. DALECKY: Not only electronic, but an

3 official version of the Federal Register.

4   MR. WASH: Okay. And there's the XML version

5 of that that we've created that is referenced on

6 data.gov. So I think the question that Selene's use

7 case was leading to is the fact that the XML is

8 referenced on data.gov, system B I think in your

9 example right, when it references back to us system A,

10 do we have responsibility for the data.gov

11 representation of that data if it were to be authentic?

12 Is that something that you all would expect GPO to be

13 responsible for in that chain from system A to system B

14 where users may go to system B, data.gov, to get access

15 to that data? Is it our responsibility?

16   MR. HORTON: Bob Horton, Minnesota Historical

17 Society. Maybe not the right analogy, but I run an

18 archive in the library and all sorts of people come in

19 and use the material there. I take no responsibility

20 for what they do with it. I mean is that similar to

21 what you're saying? I mean you're making this content

22 available for use, interpretation, re-use, mashup. I

1 don't see how you could hope to manage it any kind of

2 reasonable way.

3   But it then becomes the responsibility of

4 some, you know, tertiary user, somebody who's gone to

5 that intermediary, used it and then wants to trace it

6 back. But that's his or her own decision to whether,

7 you know, to sue somebody for libel or do some more

8 research or write another book. I just don't see how

9 you could take that on, that responsibility.

10   MR. DAVIS: This is Rick Davis, GPO. From a

11 policy perspective, I would see it at minimum that if

12 we make that data set available in XML format and it's

13 put on data.gov, it's mashed up by another user or

14 another third party, at minimum there would be an

15 interest in going back to that chain of custody issue,

16 tracing back to where the original data came from. Was

17 that information authentic that I worked with to

18 mashup.

19   But going back to Mr. Shuler's question,

20 traditionally when GPO has disseminated that

21 information then it's up to the user to make any use of

22 it as they see fit.

81

1   MR. HANNAN: This is John Hannan from GPO. I

2 think that's a useful model. I think we kind of, you

3 know, see that really as probably about the only

4 practical way to keep furthering this. But it's

5 interesting, it's an interesting discussion.

6   MR. SHULER: I just don't see anything

7 inherent in the technique that we're discussing that

8 suggests that GPO's relationship with its products has

9 changed significantly enough to alter the no copyright

10 traditions, if you will.

11   MR. HANNAN: There's no intent to change any

12 of that. We're simply looking to facilitate things in

13 an electronic world that are useful to the community.

14   MR. SHULER: When you're saying custodial, I

15 mean when you enter the concept of custodial into the

16 discussion you then enter that idea of control over

17 secondary, tertiary fourth uses and so on.

18   MR. HANNAN: So, okay Selene did you

19 introduce custodial? Only kidding, because

20 (inaudible). I think it's a good -- again that's the

21 purpose of today's dialogue is to explore different

22 facets of this and to help inform our decision making

1 as we go along about how to (inaudible) systems to the

2 best (inaudible).

3   MR. YU: I just want to get a clarification

4 about the semantic meaning of what it means to

5 digitally sign data. So is the assumption that GPO

6 will only sign a data set if it considers it the

7 official version? You know, official version of the

8 Federal Register and only when it's official will it be

9 signed? Or does it mean, you know, we're putting this

10 out unofficially on data.gov, it's still being

11 published by us and it hasn't been modified in transit,

12 will you guys still sign those documents? So I mean an

13 associated question is, you know, if in the data.gov

14 workflow, if somehow instead of the data being hosted

15 by each agency, it was hosted centrally and any time

16 you uploaded a data set to data.gov it automatically

17 got digitally signed in the workflow, would agencies

18 potentially be less willing to put data on there

19 because they would feel like putting something into

20 data.gov would somehow make it more official because it

21 was now signed?

22   MR. HANNAN: Well I think that's exactly the

1 purpose of today's dialogue. Those are great

2 questions. And we certainly don't claim to have all

3 the answers at GPO. We want to accept a lot of input

4 and perspectives so that we can help to guide what we

5 do to help make it the best for the community overall.

6   I think the concept of, you know, a digital

7 signature obviously takes some effort and some time and

8 so when that's applied at GPO it's usually for the

9 purpose to provide something that's more reliable in

10 some ways. But I'm not sure I would state it or go,

11 you know, to phrase (inaudible) your question.

12   MR. YU: Yeah, because I mean to go to a

13 specific example. I mean I've talked to Mike Wash

14 about this before with the XML version of the Federal

15 Register. And I mean it always seemed to me like

16 because the XML version may or may not be an exact

17 replica of the content in the PDF version, you guys

18 aren't willing to sign it because you're not sure yet.

19 But the signing actually provides, you know, a level of

20 reliability, as you say, even if it's not, you know,

21 the official that, you know, is legally representative

22 of the Federal Register.

1   MR. HANNAN: Yeah, so I think great comment

2   and we're going to talk a little bit later about if we

3   were to think about how to apply authentication in an

4   XML arena, what are some of your feelings about some of

5   the input, some of the criteria. And then what would

6   that, you know, "mean." Those are policy oriented

7   things that, for the specific case of the Federal

8   Register, obviously the Federal Register has got a lot

9   to say about what that really means. So, yes Harold.

10   MR. BOOTH: Harold Booth. Just to kind of

11   add on to Harlan's comment. You may want to establish

12   different types of signatures or certificates for

13   different purposes, you know, to establish -- one

14   source semantic meaning and then -- that which would be

15   the official version and then you could have another

16   one just to establish titles, so it doesn't have to be

17   an either or choice on your part by any means. You can

18   still use the same framework that you've been --

19   technical framework that you've established.

20   Another thing, as an outsider to your

21   community, one thing I'd like to just mention, you're

22   trying to establish digital means of doing something

1 you're already doing in the real world. Maybe it would

2 be useful, as you talk about this issue, you talk

3 through how you do it in the real world today in a

4 printed manner and then just kind of say, "Okay, well

5 what's the analogy, or what's the analogous process or

6 step that we would need to do in the digital realm."

7   MR. HANNAN: Great. That's great input.

8 That's the only way I can, you know, make any sense out

9 of this myself. I totally agree, I think those

10 analogies are really often times they're useful for

11 (inaudible).

12   MS. RUSSELL: Lisa Russell. I don't think

13 it's working.

14   MR. HANNAN: Maybe the battery's dead.

15   MS. RUSSELL: I was using the wrong switch.

16 Lisa Russell, GPO. What we've been doing with

17 authentication to date is that when there's something

18 that we want to authenticate we go to the originating

19 agency and talk to them and say, "Hey, is it okay if we

20 originate your stuff?" And getting at that official

21 issue we've had some agencies where, you know, like we

22 got permission to sign the U.S. Code on FDsys however

1 in order to do that we had to agree that we're not

2 saying that this is official, that they can use it a

3 court of law. What we're saying with that is that

4 we're putting a signature on it and it indicates to the

5 user that it has not been changed. You know, it's come

6 through the official channels and it has not been

7 changed, but no this is not -- we're not saying this

8 official, that you can take it to court.

9   So we worked through a lot of those issues.

10 And we've also looked at -- you know, we've looked at

11 do we use different -- you know, we use a blue one in

12 this case and a pink one in this case, those types of

13 things with the signatures and that gets a little bit

14 tricky. And we've also looked at -- you know, people

15 have talked about we want to put numbers on them and

16 say, "This is -- this has official level one, this is

17 level two, this is level three," that gets a little

18 tricky when you start looking at some of the older

19 stuff. Is something that's been on the shelf in a rare

20 books room in a library more official or less official

21 than something that was taken directly from an agency's

22 website which may or may not have been hacked.

1   So you know, it gets tricky. I think there's

2 an argument there, which is a one and which is a two

3 and when we start putting those numbers on it people

4 start getting a little bit confused.

5   MR. HANNAN: Yeah, I would just add, this is

6 John from GPO, that I think that's the purpose of

7 today's dialogue is to try to get some feeling about

8 how it might be useful to interpret these kinds of

9 questions going forward, because there isn't a lot to

10 really guide us, quite honestly in this regard, to your

11 question, Harold. That's why I think we want to get

12 the widest range of input we can so that we can make

13 good decisions and kind of use some of these electronic

14 capabilities that are becoming more practical to use.

15   All right, so everyone's -- let me think

16 about how to get at this again which is we tried this

17 because I think the question that one of the things

18 that we had as desired outcomes was to try to get a

19 feel for was the concept of a hash-based, pick one

20 method that might be lower weight, less processing

21 intensive, is that a useful thing that's needed by

22 parties in the system that we should think about

1 providing through our electronic dissemination channel.

2 Any thoughts or -- I mean has anybody really got to

3 have that or -- yes, Steven?

4   MR. ANDERSON: Microphone, please.

5   MR. HANNAN: Is it on?

6   MR. ANDERSON: It is on. Steve Anderson,

7 Maryland State Law Library. During the break one of

8 the questions that came up was in a locks type world

9 where you have other duplicates of an original, it

10 seems like having a hash-based method for official

11 copies would be reasonable. What I don't know, I mean

12 getting getting back philosophically is how many

13 original authenticated copies one might want. If one

14 only wants to have one authenticated original that's

15 great and then you use the, you know, digital signature

16 for that. But if the world that's envisioned includes

17 official duplicates, then it seems like that would be

18 very easily handled by a hash-based method.

19   Of course techies could probably correct me

20 with all of this, and they're more than welcome to.

21   MR. HANNAN: Well I think -- this is one --

22 just to jump in, that's really the question isn't it?

1 It's like if you're going to provide a less robust

2 means why are you doing anything with it? Why isn't it

3 just available? So given that the other channel is a

4 more, you know, robustly authenticated piece of

5 material that could be used.

6   I mean I think that's really the interest

7 question that we're trying to get a hand on, because

8 clearly having multiple methods costs more, is more

9 complex, more things can go wrong. So if the concept

10 is that there's a light weight method that brings

11 value, you know, why would it really be needed if the

12 file is there already to be used and you could rely on

13 a more robustly authenticated available electronic

14 version if some question came up.

15   It's just a question, I don't -- I'm not

16 saying right or wrong or anything, but that's maybe

17 something that you have some input on.

18   MS. DALECKY: Selene Dalecky, from GPO. And

19 I think one thing to look at in terms of what methods

20 are needed, I guess how much security, how much comfort

21 do you need with a data set. Does that determine the

22 method as well? For example, if we're looking at a

1 data set that is unofficial, that is something that

2 people are going to be reusing and mixing with other

3 content or taking portions of for you know,

4 informational purposes only, not for specific legal

5 purposes or it's not going to be cited, is that

6 something where just a dump where the hash has taken

7 place and you can show that when it's transferred from

8 this system to the next system? Or if you've pulled

9 out the data set you know that it's been securely

10 maintained in a repository that has security controls

11 around it, is that enough as opposed to you need to

12 take any file somewhere and cite to it and point to it

13 as the official version that you need to use for some

14 matter of recourse?

15   MR. YU: Yeah, I mean I think you know, hash-

16 based methods obviously don't get you everything, but

17 you know, as we said earlier, you can piggyback on

18 existing security mechanisms. So you know, if you

19 publish the hash on a secure website, on an SSL https

20 website then you know, somebody could take that hash,

21 know it's actually from the GPO and then do the

22 integrity check with the downloaded data set that they

1 have.

2   I think the tradeoff is, you know, when you

3 do cryptographic digital signatures you might have a

4 system that's sort of all in one, possibly an easy user

5 interface, whereas if you sort of compose these various

6 pieces together to create the system you want, you just

7 don't have easy tools for people to, you know, do the

8 checks and to do the verification. It's possible, it's

9 just not easy.

10   MR. HANNAN: Right. I think that is the

11 challenge, that's right.

12   MR. MAYER: Jonathan Mayer from Stanford. I

13 guess I would also add to the extent that with some of

14 these algorithms, not all of these algorithms a hash-

15 based method would be subsumed in a cryptographic

16 digital signature, then you can facilitate some user

17 choice there. So if the user doesn't really care too

18 much to actually go to the computational trouble of

19 checking the signature then they can only check the

20 hash. And if the signature's important they can take

21 that additional step.

22   MR. HANNAN: How do others feel in the room

92

1 about the usefulness of that second kind of a channel?

2 Useful, make use of it, don't care?

3   MR. SHULER: John Shuler, University of

4 Illinois at Chicago.

5   MR. HANNAN: Yes, John.

6   MR. SHULER: Speaking from the users that

7 I've been dealing with for the last few years, I would

8 say the authenticity comes from situational rather than

9 technical. They're coming to an official depository,

10 supposedly they're talking to an authentic librarian

11 who's working within that depository. The items have

12 associated with them all these bits and pieces that

13 say, these quote/unquote are "official publications"

14 both digital and paper. And for 80 percent of the

15 people that I deal with, it's good enough. They don't

16 need to go back and do the due diligence, they don't

17 need to go back and assure custodial chains of

18 responsibility.

19   So the question I would ask you, and this is

20 a culinary to my earlier question, what's driving your

21 question? Who are you trying to serve by asking the

22 question? I'm reminded of the old phrase, "when you

1 hammer every problem's a nail," what's the problem that

2 you're trying to get at? If you're talking about the

3 users I deal with, hash marks, digital signatures not

4 so much, really don't care. But if you're talking

5 about the legal community, if you're talking about

6 other people that have a much more intimate like with

7 where this information came from, I would say it's a

8 huge concern.

9   It's about where does the majority of your

10 business lie which be the question.

11   MR. HANNAN: Right. Yeah, no that's great.

12 Thanks. Can we get a microphone?

13   MS. SEARS: Suzanne Sears, University of

14 North Texas. I would agree with John to a point that

15 yes, most of the users that come into my library,

16 they're not asking me, "Is this authentic," because

17 they're making the assumption it is. When they come

18 into the library they're assuming that as a librarian

19 I've already vetted that source and that I'm giving

20 them a reliable source.

21   So I think that, you know, yes we need to

22 have it authenticated on your end so that when we're

1 purchasing -- I was talking to Steve earlier, you know,

2 just when we purchased a book, if we purchase an

3 Encyclopedia of Political Science we're going to make

4 sure that its from a reliable source, a reliable

5 publisher, somebody who has authority in the field.

6 We're going to do the same thing with the depository

7 material. If we know that chain of custody is really

8 important to us, is it coming from the federal agency,

9 is it authentic, before we present it to our users.

10   And I do think that we've built up the trust

11 in the community that they're not asking that question

12 because they're already assuming that if we're giving

13 it to them it is official.

14   MR. HANNAN: Thank you. That's really good

15 info.

16   MS. BAISH: Although in 2010 people aren't

17 always -- you can turn off that one. Well this is 2010

18 and we're all struggling to keep our print library

19 collections because more and more people are accessing

20 information coming from FDsys and GPO Access, going to

21 the Department of Labor website, going to the Senate

22 website. And so I mean in terms of your authentication

1 and the mission of this agency, that's where AALL sees

2 your importance and totally supportive of your

3 description of what FDsys is.

4   In other words, you are as you did in the

5 print world, the agency for informing the nation and

6 insuring the permanent public access and the

7 authentication and the preservation down the road. The

8 challenges of course for you are we're now, in a

9 completely decentralized world of federal government

10 information and how do you redefine your role. And

11 we're looking to you actually to do that and solve

12 these problems in some way.

13   I think that the discussion about, you know,

14 is there any authentication that is totally portable,

15 verifiable that moves within that document is -- should

16 be the ultimate goal of the agency. But obviously

17 we're restricted to current technologies.

18   MR. HANNAN: Thanks, that's great. Well I

19 think that's something that may be kind of loops back

20 to what Harlan said earlier about -- and this is very

21 much on our minds, is that the decisions we take, we

22 don't want to take decisions that have incentives for

1 there to be less of the workflow involved, in terms of

2 both agencies using our capabilities and services or

3 other data.gov resources. We want to take decisions

4 that help facilitate the movement in an authentic way

5 of these electronic materials.

6   So that's an important concept, I think, for

7 us at GPO. And so this workshop is a way to try to get

8 at will certain techniques hinder, set up incentives

9 that won't have as much information being facilitated

10 with parties that we've always done business with. So

11 I think that's a great -- that's something that's

12 really important to us.

13   Other comments? Thank you.

14   MR. HORTON: Just briefly, Bob Horton from

15 the Minnesota Historical Society. I wanted to echo

16 what John was saying, maybe emphasize it a bit more.

17 I'll give an example. Years ago Minnesota published or

18 passed a law on establishing digital signatures and

19 certificate authorities. And I happened to be sitting

20 next to the ABA representative at the committee hearing

21 and he muttered to me that, you know, this is too much

22 for the little things and not enough for the big

1 things.

2   And I think that's something you should keep

3 in mind is that maybe 80 percent of the people don't

4 care all about this, and the people who really care

5 will probably be able, you know, like O.J. Simpson's

6 lawyers in the D.N.A. trial, blow a hole through

7 whatever you do because it's not as simple as attaching

8 a signature to a single document, you've got a whole

9 variety of business rules and connections and

10 partnerships and relationships that you're going to

11 have to document and define if anybody asks any really

12 probing and substantive questions. So, you know, maybe

13 this is a -- maybe that makes it a little bit more

14 complicated, but I do think whoever said -- I believe -

15 - I would say it was Kate, I mean there's a metadata

16 and there's a business rule approach to this that is as

17 important, maybe even more important than the

18 technological wrapper you're using for your

19 transmission.

20   MR. HANNAN: Yeah, great comment.

21   MR. MAYER: Jonathan Mayer from Stanford. I

22 wanted to respond on the point about whether users care

1 or not. I guess I want to offer a brief comment, kind

2 of in defense of the user. And that is I don't --

3 can't speak to every user of course but I think there's

4 an important role here in that there is a chain of

5 trust. Right? So if you use, let's say Google

6 Patents, you're trusting in Google and you're trusting

7 Google got their material from the Patent Office. I

8 think we're pretty comfortable with trusting those kind

9 of intermediaries every day. So to the extent a

10 consumer is looking at a mashup of GPO data I think

11 they do have some measure of confidence, let's say

12 whether looking at a mashup made by the (inaudible)

13 Foundation instead of you know, something like

14 ThisIsAMadeUpMashup.com. They have some means of

15 judging, it's not perfect but I think the situation's a

16 little bit rosier than had been suggested.

17   MR. HANNAN: Thanks. Anybody else from GPO?

18 Any other thoughts? Thanks, this was really good

19 discussions, great viewpoints. Thanks for sharing

20 that.

21   So let's go ahead and -- we're probably right

22 about lunchtime honestly. So I think what we --

1   MS. DALECKY: I did just want to kind of

2   close up with one more --

3   MR. HANNAN: Oh, please. Yeah, sure.

4   MS. DALECKY: -- just to kind of bring back

5   what we were just talking about, in terms of overkill

6   versus not enough. In the case of FDsys now or when

7   we're bringing in more content from various sources, if

8   we have a documented, secure content management system

9   that follows best practice guidelines that can meet

10 audit standards, the content that we have is secure.

11 But if we can also show from an input process that when

12 we are actually bringing content into the system, we've

13 secured that channel as well and we know who's putting

14 in the content and we know where that content is coming

15 from originally, so it's a deposited content from a

16 born digital content from an agency, or it's a

17 converted file that somebody from the Library of

18 Congress is providing us, so we've secured those

19 channels and we can show that, we can demonstrate that

20 through our audits and our documentation, then the

21 question becomes what level does that need to be

22 conveyed to users. And I think that's the 80 percent

100

1 don't care, it's enough to know it's coming from GPO.

2 And the 20 percent, well it needs to be very clear all

3 that you've done, you know, succinctly showing any

4 signature or something that we can then present to

5 somebody who needs to know this information.

6   And then how much needs to be beyond that?

7 How much is knowing where it's coming from and how much

8 is the content itself? How does it -- does it have to

9 persist with the content in the form of a signature on

10 a PDF or can it be enough to know that this content

11 came from a source that can prove that when you got it

12 from our source it has been maintained and the chain is

13 there and it hasn't been broken.

14   And I think in terms of looking at system A,

15 system B to the end user or some of these other use

16 cases that that really boils it down. Is how much of

17 the security is knowing where it came from and being

18 able to present where it came from, and how much of it

19 is the content itself persisting with that content

20 being handed down from the system to person to person.

21   MR. HANNAN: So is that a question to the

22 audience, Selene?

1   MS. DALECKY: Yeah, I think it's just kind of

2   something to think about and say, "Well what is most

3   important and in what case?"   Again, is it enough and

4   80 percent of the time, just to know where it came from

5   originally and that's enough, or do we have to persist

6   the authentication of the content itself and make sure

7   that everybody knows that that content is still good

8   and hasn't been altered you know, time and time and

9   time again as it passes on from system to system or

10 person to person.

11   MR. HANNAN: I don't think we can answer our

12 question (inaudible). Lisa, I'm just kidding.

13   MS. RUSSELL: Lisa Russell, GPO. Just sort

14 of a related thing. I think we've been talking about

15 different users needing -- wanting different levels of

16 authentication. I think sometimes the same user wants

17 different things in the same situation -- in different

18 situations, because once we started signing the bills

19 we started getting questions from users who were

20 saying, "Hey, I used to be able to download your file

21 and make notes on it for my own use. I can't do that

22 anymore. What's going on here? Can you fix this for

1 me?"

2   And there is actually a way where they can

3 save a copy that does not have the signature on that

4 then they can make it, but in that case, you know, when

5 they're getting from us they want that assurance that

6 this is good, this is the correct version, but then

7 they want to be able to use it for their own purposes

8 and tweak it and so on. But then we also want to make

9 sure that they're not going to be able to pass that off

10 as an official version. So I think there are some

11 other issues there maybe that the same user might want

12 different things in different situations.

13   MR. HANNAN: That's a great point. I would

14 tend to say it's pretty clear that, you know, if there

15 was no cost and it was an ideal world, obviously we

16 would have, you know these multiple channels. And I

17 think that we're going to work hard to think about, you

18 know, what is the marginal effort and complexity of

19 doing that. Based on the discussion here it sounds

20 like there might be some interesting value to come out

21 of it.

22   I think the concept of, you know, mashups is

1 an interesting one that's probably beyond the scope of

2 what we're doing today. But we'll continue that

3 conversation on that once we learn how to walk.

4   So I don't want to cut anyone off. Does

5 anyone else want to chime in or address what Selene

6 talked about? If not I think this is a good time to

7 break for lunch and then come back at one o'clock and

8 we'll keep plowing through this material. And I hope

9 this is useful. Does that sound good to everyone? I

10 think this is a good time to hit the cafeteria before

11 it gets really crowded.

12   So with that we'll break till one o'clock.

13 Thanks.

14   (Off the record)

15   MR. HANNAN: All right. I think we're all

16 back. Thanks. I hope everybody got something decent

17 for lunch. And to kick off, to get back into this

18 exciting topic -- so what we'll do at this point, Ted's

19 making fun of my usual --

20   SPEAKER: I do like that. From lunch,

21 exciting topic.

22   MR. HANNAN: Yes. Let's go into some

104

1 questions and some areas that we want to get your

2 feedback on related to authentication of things beyond

3 the files, which is what we'll do today. So on slide -

4 - on 12 in your packet, you'll see a little bit of

5 observations from our end. Thanks, Jessica. We went

6 ahead and just got going. You haven't missed anything.

7 So this slide is observations.

8   So and one of the things that has been

9 brought up by those is -- well, for content types or

10 BETA formats other than PDF, maybe we could use PDF as

11 a carrier, which it certainly is technically capable of

12 doing, to encapsulate other file types, like XML, text

13 files, ASCII text, whatever it is.

14   The disadvantages for that, there are some

15 disadvantages, which is that those embedded files don't

16 have direct authentication, they kind of inherit the

17 authentication of the PDF carrier. And how do you link

18 all that standard information with the authentication

19 of the overall file to the [inaudible] file as well?

20 There's not a lot of standard ways of doing that yet. A

21 lot of people have ideas, but they're just -- so my

22 conclusion right now is probably the best option is

1 we're examining other options. That's what I'd like to

2 get your input on.

3   So when we think about all the -- high

4 volume, system-to-system processing applications, we

5 inevitably, it seems like, start talking about XML data

6 or, potentially, binary data. So there are a couple of

7 just high-level options, just from the technology side

8 about thinking about this. Both of these formats, the

9 first one, which is XML, and the second one, which is

10 the traditional PKCS7 wording and concept, a lot of you

11 have unambiguous digital representation of some data.

12   And so I guess we'd like to see if you guys

13 have any feedback either way, realizing this is a very

14 technical question. It may be something that you just

15 say, let's go to the next slide. But it seems, to us I

16 guess it all makes sense because we're in such an XML-

17 oriented world in many respects, and there's been

18 things in GPO with respect to the Federal Register

19 where XML is already a type of final that we're

20 disseminating.

21   So it seems like XML's the right thing, but

22 we wanted to get your feedback too, so that's really

1 how we're going to open it up to the audience at this

2 point. Unless, Ric, did you want to jump in?

3   MR. DAVIS: Yeah. Ric Davis, GPO. I don't

4 think this one's working right now. Ric Davis, GPO.

5 One thing to consider on that is, in addition to the

6 signing process of native files, is also the net effect

7 on the end user. Because I think we talked about this

8 at the beginning of the discussion. One of the reasons

9 we chose the process that we did was not to require for

10 the end user difficult third-party plug-ins to be able

11 to make use of our authentication processes.

12   And as John mentioned, right now, you know,

13 we can take native file formats and put a PDF wrapper

14 around them and make those available. But, ideally,

15 what we've heard through use cases is users want the

16 ability -- us to have the ability to sign those native

17 files. But on the other end, they want the same ease

18 of use that they have with the PDF to be able to do

19 validation.

20   And, again, I think this is where,

21 inevitably, we talk about like the two basic ways to

22 segment the users who may be interested in this data

1 for GPO, individual users, citizens and then large

2 intermediaries or system-to-system processors. So any

3 feedback at this point? Mike --

4   MR. GALLUCCHIO: This is Kevin Gallucchio

5 from Department of Defense. So you've asked the

6 paranoid guy again. And I would caution you against

7 using PDFs because they have a lot of kind of nasty

8 things in them, like hyperlinks, and you could run --

9 include executables and all sorts of attachments that

10 you really don't want on your computer.

11   And in a standards -- from a standard

12 developing point of view, the PDF kind of attachments

13 is really kind of an afterthought functionality that

14 they added after the specification was built. So what

15 is XML, is kind of a much better way of supporting

16 extra data and files and things like that. So I would

17 say XML or even the MIME attachments or things like

18 that would be much better. You can write applications

19 that handle these -- it's trivial because you have

20 these packages that can extract -- go to different

21 parts of an XML document, you know, and say, you know

22 what?

108

1   Give me this path, give me the element, you

2   know, that's located at this path, and it's very easy

3   to handle for [inaudible] whereas with PDF, you're

4   going to be tied to Adobe a lot, or you know, you've

5   got to develop something specific to PDF, and that's

6   going to be a bit harder, I think, in my opinion. So --

7   MR. HANNAN: Thanks, that's good. Others at

8   this point? Or we can just keep going along. Okay.

9   Let's go to the next slide and see if this -- so the

10 next set of slides talk about native XML

11 authentication, assuming that that's kind of of

12 interest, because as I say, we're already disseminating

13 some XML, so we are thinking about does it make sense,

14 and if it's valuable, and then how would we think about

15 doing authenticated XMLs, so these next few slides talk

16 a little bit about different ways to do signing and

17 digital signatures with XML.

18   And there are, basically, three different

19 types, envelope signatures, enveloping and detached

20 signatures. The pros and cons we'll talk a little bit

21 about in the following slide so if we can just go to

22 that.

1   I did have a graphic of pictures here which I

2 wish I'd had, but maybe we can post something on a web

3 page after this. So an envelope signature is the

4 concept where the signature is embedded inside the

5 file, sot he signature is a child, essentially, of the

6 content or the file itself. It's inside the file. The

7 document or the file needs a placeholder to hold one

8 signature or multiple signatures.

9   So the advantages are everything's right

10 there in one place. This is, essentially, the PDF

11 concept. Offline validation facilitates that

12 verification, kind of more readily facilitates that or

13 it does facilitate it. The signed and the unsigned

14 content, they end up being kind of in the same format

15 as it turns out. That could have some useful features

16 to the practicality, ease of use downstream.

17   Enveloping signatures, this is the concept

18 where the signature is really kind of a parent of the

19 content. In other words, the signed content is kind of

20 underneath the signature itself. So when you first go

21 to open the file, your software has to be smart enough

22 to know how to deal with the signature right off the

1 bat because that's kind of the overarching -- it

2 envelopes the whole thing.

3   That has pros and cons relative to existing

4 software tools and how cheap they are, how readily

5 available they are, that sort of thing.

6   Again, the signature and the [inaudible] are

7 very much coupled together. It's just kind of a

8 different way to orient them. But the signed and the

9 unsigned content have different formats. Sometimes

10 that's a little more complicated. Potentially, it

11 means you have to have two viewers, not just one. So

12 the unsigned raw content has got the different format

13 than the signed stuff. Not that that's right or wrong.

14   Detached signatures, the signature is

15 completely separate from the content. The processing

16 of the signature and the document are separated.

17 There's no difference at all between the signed and

18 unsigned content. They're exactly the same. It's this

19 second step you're doing with another piece of digital

20 data somewhere that will determine what you're going to

21 think about that content.

22   You know, when you start thinking about mash-

1 ups of -- separate documents, in this content, I think

2 it actually starts out with some advantages to it in

3 some ways. Disadvantages are that you've got a link.

4 You've got to have a process to link the content and

5 signature together. There really aren't any standard

6 protocols for this yet. I'm sure there will be at some

7 point. Therefore, they tend to be higher costs, it's a

8 lot more coding experiences.

9   Some of the same disadvantages as you have

10 with the embedded files in PDF come up in this context.

11 And lastly, kind of -- some of our observations in

12 thinking about this was since the signed and the

13 unsigned content are exactly the same, it can be quite

14 easy for users or parties involved in the process to

15 become confused about what really is or isn't actually

16 the content that is important.

17   MR. WASH: Is there an example of the

18 attached signatures available today?

19   MR. GALLUCCHIO: That's a great question. I

20 don't really know of any practical systems that are

21 used for anything but I may not just be aware of it.

22   MR. WASH: So where does surety fit in of

112

1 these three examples?

2   MR. GALLUCCHIO: They're in -- they're not a

3 signature but they're in that class --

4   MR. WASH: Where the --

5   MR. GALLUCCHIO: Yeah, it's a detached

6 methodology --

7   MR. WASH: For the encrypted signatures, this

8 is detached --

9   MR. GALLUCCHIO: Yeah. Yes, sir.?

10   MR. YU: This is Harlan for [inaudible]. I

11 don't really think it matters all that much whether

12 it's enveloped or enveloping or separate. I mean, the

13 people who are going to be using X mobile data, they're

14 going to be developers who know how to use command line

15 tools. They can find that signature and apply it to

16 the data as long as there's a specification for what

17 that data is and how it's attached. The W3C has a

18 standard for XML signatures, and maybe we should just

19 use that.

20   MR. HANNAN: All right. That's great input.

21 Thank you. And that's, I think, an interesting

22 viewpoint. Let's try to go, if we can, let's go

113

1 through this which tries to summarize some of our

2 conclusions to this point, and that will be a great

3 jumping off point for just what you've laid out.

4   So, you know, our current approach uses

5 envelope signatures. In some ways, it seems practical,

6 might be [inaudible] XML world. For the cases in which

7 there are multiple signatures, then this is, by far,

8 the simplest method, but again, we're going to talk

9 later about -- on the other hand, there are things that

10 are applied by -- signatures or, in the case where you

11 do have multiple content signers.

12   The next item really speaks to that. So when

13 you do consider the case where you have multiple

14 signers, you want to try to use a way to do chain of

15 custody using these kinds of authentication techniques.

16 There are other ways of doing that too, as in meta

17 data.

18   But when you're doing it just with these

19 techniques alone, trying to convey chains of custody,

20 an envelope signature approach requires a common

21 specification. You absolutely must have a common

22 specification for the document and try to find some

114

1 reasonable upper limit about how many hands it's going

2 to go through.

3   The -- XML requires a lot of coordination

4 between GPO and content originators anyway as it is. We

5 already coordinate quite a bit. Maybe that's not such

6 a big issue, but it certainly is applied by the

7 envelope signature process.

8   When you start thinking about chain of

9 custody, it seems like it's more complex to use

10 enveloping or the detached signature methods, more

11 complex for the protocols and the software involved. So

12 maybe we should start with envelope. If we're going to

13 do this and it's of value, we can start with envelope

14 and see how it goes.

15   That's kind of conclusions to this point. So

16 we want to open it up to you. I realize this is pretty

17 technical -- but to see what you're thinking is, do you

18 care one way or the other, do we have -- for those,

19 especially those that are really interested in, you

20 know, straight-through XML processing, for instance,

21 and you know, high-volume, hands-off, no human involved

22 in it orientation. So let's start with you. Do we

115

1 need the mike?

2   MR. ANDERSON: That's fine. I think

3 everybody can hear me.

4   MR. HANNAN: Okay, yeah.

5   MR. ANDERSON: Steve Anderson from the

6 Maryland State Law Library. Your comment earlier that

7 GPO is not a standards body would seem to preclude the

8 usage of the -- which one was it -- the detached one

9 where there was no formal standard to govern the

10 detachment or reattachment process.

11   Simply because in that scenario, then, you

12 would have to be developing -- you would have to

13 develop a standard to do that. And if you don't want

14 to be a standards-creating body, then don't use that

15 method.

16   MR. HANNAN: I think that's a great comment,

17 I think, and we appreciate you voicing that.

18   MR. ANDERSON: Just trying to make it easier

19 on you.

20   MR. HANNAN: Yeah. I think that's some of

21 what has become apparent to us, but again, we want to

22 try to validate that. So thanks, that's great,

116

1 Stephen. Well, John, are you next? Did you want to

2 go? We'll let Harold go then.

3   MR. BOOTH: Harold Booth. Just to add on --

4 maybe to re-complicate your life again rather than

5 trying to simplify, but the fact that you're creating

6 XML documents is, in effect, you are creating

7 specifications or standards for those documents. At

8 the end of the day, you are doing that. So when you

9 embed that signature as part of that format, however

10 you do that, you are, in effect, creating that

11 specification standard, however -- the terminology you

12 wish to use.

13   I will add on that when we're talking about

14 detached and the definition within W3C, having a

15 sibling element signature block is equivalent to

16 detached. It doesn't, necessarily, need to be a

17 separate document, per se. It just needs to be -- so

18 if I have -- and I know I'm getting technical, and I

19 apologize to anyone that's not familiar with XML, that

20 if you have a signature block, it's a sibling to the

21 thing that's being signed, that's considered detached

22 within the vocabulary of the W3C signature standard,

1 just to be clear.

2   It doesn't, necessarily, mean that they're

3 separate documents. So if someone was asking for an

4 example, often times with open-source software, they

5 will have a separate cache file that's separate from

6 the executable that you're downloading. That would be

7 another example of detached; that would be two

8 different files that you have to manage and maintain

9 separately.

10   MR. HANNAN: Okay. Thanks. And we'll update

11 our materials and try to be more precise with that.

12 That's a great comment. So --

13   MR. MAYER: I want to build upon Harlan's

14 comments. I guess this morning I kind of made the case

15 against the apathetic user. I now kind of want to make

16 the case in favor of the apathetic developer. At base,

17 you need to store some signatures and what they're

18 signing. You can store them at the beginning of a

19 document, you can store them in the document, you can

20 store them in another file.

21   But from the developer's perspective, they're

22 going to load these in and check them. I think the

1 real considerations that come to mind are if there's a

2 software library or several good ones available for

3 some of these, they seem to have some widespread

4 support that would tilt in favor. Similarly, if there

5 are particularly bad libraries where it's really hard

6 to manipulate, one of these PDFs come to mind, it's

7 notoriously quite hard to programmatically interface

8 with, then that would be kind of thumbs down on it.

9   MR. HANNAN: Thanks. That's good info.

10 Others have anything at this point? I realize this is

11 a pretty technical area -- oh, thank you. Kevin?

12   KEVIN GALLUCCHIO: Kevin Gallucchio from DOD.

13 It's just that the -- I just want to warn you that the

14 enveloped approach is kind of the most radical for --

15 you won't be able to ramp up, whereas the detached is

16 like the least amount of work. You'll be able to have,

17 like, files that have detached signatures next to files

18 that don't. This is not -- that might be a plus or a

19 minus.

20   But hardly anything in government starts, you

21 know, as one set. Everything's compliant. Usually we

22 ramp up, at least in the DOD. I don't know, maybe in

1 your part of the government, it works smooth. But we

2 ramp up, so detached would be the easiest, enveloping

3 second easiest, and enveloped the hardest.

4   MR. HANNAN: The hardest, because of that

5 having to have the common specification for --

6   MR. GALLUCCHIO: Yeah.

7   MR. HANNAN: -- things go. That's good,

8 that's great input, thanks. That's really good. Others

9 at this point, or ready to keep moving on and get

10 through this? So, Harlan, if I -- just one quick

11 comment. If I was going to summarize your input, it

12 doesn't matter as much, just any one of them might be

13 okay.

14   MR. YU: Yeah. I don't think there are huge

15 technical advantages or disadvantages. It just

16 depends, as John said, the available tools and what

17 people are used to. As long as people know what to

18 expect, I think it's --

19   MR. HANNAN: Right. Harold, in this, do you

20 have any -- you've already given us some good input on

21 this. Do you have anything that we ought to think

22 about again, those three, which ones we're going to

1 choose? Given that we know we have lots of straight-

2 through system-to-system users, but also --

3   MR. BOOTH: I have nothing to add with

4 respect to which one you should choose. I think,

5 ultimately, that's -- again, from the feedback you got,

6 there are pros and cons to each of them again. So it's

7 more, I think from your end, how difficult it is for

8 you to manage and maintain that, I think, is really the

9 decision that you, as an agency, need to make.

10   The one thing I would caution is, you know,

11 as I'm starting to dig through and implementing this

12 within my own space, there are numerous issues with XML

13 signing. And, again, I'm going to get very technical,

14 and I apologize to anyone that doesn't -- isn't

15 terribly interested in this.

16   MR. HANNAN: That's okay.

17   MR. BOOTH: There are -- the W3C has

18 recognized this. There are a series of best practices

19 that -- technical papers they're trying to produce, and

20 there are security issues that, as people need to

21 validate or sign data, you need to be very much aware

22 of because of the very nature of XML signing. And

1 these issues don't, necessarily, exist in some of the

2 more -- the RFC that you referenced before, the PKCS7s

3 type standards. And I'm not going to enumerate them

4 all. They do exist. I just want to, I think, raise

5 your awareness that they do exist.

6   MR. HANNAN: Thanks.

7   MR. BOOTH: And I'm more than happy to -- I

8 can give you a link to all those various resources.

9   MR. HANNAN: That would be great. I think we

10 -- I would probably take you up on that, so that sounds

11 -- that's great information, so thank you. Okay.

12 Before we leave this one, real quick, I think to

13 summarize this, it seems to us that, at GPO so far,

14 that if we decide to try to offer authentication in a

15 native format, besides what we're doing today, it

16 probably would be either native XML, or in the MIME

17 oriented, you know, PKCS7 world.

18   Again, those are both definitive, binary

19 objects. And WC3 seems to be the set of standards on

20 that. I don't think there are really any others in

21 native XML at this point, but that was something I did

22 want to ask Harold, are there any other standards

122

1 besides --

2   MR. BOOTH: Not widely used. There are some

3 that have been used by some niche communities, but for

4 the most part, WC3 standard is considered the XML

5 standard. But there are others.

6   MR. HANNAN: Okay, right. That's the great

7 thing about standards, right? There are so many to

8 choose from, as somebody once said. But thank you.

9 Because that kind of what our summation too. That

10 seemed like the standard for native XML. I appreciate

11 your feedback.

12   MR. BOOTH: I'll also add that there are many

13 libraries -- not many -- there are libraries out there

14 that already have implemented the WC3 standard as well.

15   MR. HANNAN: Got you. Super. So, to

16 summarize, we're not sure what to do yet, obviously.

17 That was one of the purposes of, as we try to figure

18 that out, to have this conference and workshop, get

19 some feedback. It's been very helpful. I think this

20 will help us formulate how best to think about moving

21 forward.

22   So now, we're going to move and switch gears

123

1 a little bit into chain of custody. Use cases, we

2 wanted to use this as an opportunity to gather some

3 feedback from you on this concept. So, Ric, if you

4 have specific things you want to jump in and add into

5 this, please do so. That would be great.

6   Basically, this is about an indicator of the

7 originator of the content, in other words, getting to

8 the provenance of the material. There are a lot of

9 different ways to think about doing that, some of which

10 these technical techniques can facilitate for you. But

11 we talked earlier today, I think Kate mentioned it from

12 GPO, about meta data being just a source of this

13 information that's part of the larger signed or

14 authenticated content.

15   But with that, one of the things we wanted to

16 note is that this, from a policy perspective, we can't

17 dictate this at GPO. It requires the content

18 originators to be on board. It's really an education

19 process for those agencies, seeing the value in it.

20 We're communicating on this at GPO with all of our

21 stakeholder agencies and partners, but we just wanted

22 to make sure you all realize it's not -- we can't

1 dictate in this arena, but we'd like to facilitate this

2 because, I think, a lot of the parties would like to

3 have this.

4   MR. DAVIS: Ric Davis, GPO. And I think part

5 of that, building upon what Kate mentioned this morning

6 on FDsys is making it easy on content originators or

7 creators of information to digitally sign content and

8 establish chain of custody from the beginning of the

9 information life cycle.

10   It's interesting, when you look at what has

11 been digitally signed, fist on GPO access and now on

12 FDsys in beta format, one of the first things that we

13 signed were federal budget files from the Office of

14 Management and Budget. And I think as Reynold

15 mentioned this morning, those had full chain of

16 custody. We issued a digital cert to them, and they

17 made use of it at the beginning of the process.

18   There is an educational process that we're

19 doing with other content originators, but the piece of

20 feedback that we most often receive is, you know, if

21 they want to understand first why is it important, why

22 does anyone care, and secondly, make it easy to do.

1   MR. HANNAN: So I think -- this is John in

2 GPO. I think one of the things that might be helpful

3 if this is really an important facet of this topic for

4 you is to kind of assist in that education process as

5 you're chatting with people, that may reinforce that

6 concept. I think a lot of agencies are receptive but,

7 you know, everyone's got a lot to do, extra things and

8 changes to process are always something that people

9 don't take lightly, they have to be very careful about.

10 So let's go on to the next one.

11   Here are some factors that we just wanted to

12 throw out to stimulate some discussion, maybe. Ability

13 to view the entire chain of custody. Having that with

14 the document, that seems important, we just wanted to

15 validate that with you. Open standards, again, seem

16 like the way to go if they exist. They do for some of

17 the more fundamental mathematical techniques.

18   The chain of custody being completely

19 present, preserved with the document, that's a little

20 bit -- the first comment, but is that a valuable thing

21 to you. And for XML and PDF files, both of these other

22 methods can allow the full chain of custody to travel

1 with the document. Having embedded the meta data,

2 clearly, would allow it to -- if the meta data is,

3 travels with the file in question, then it, obviously,

4 provides that holistic capability too, which seems

5 simple in the best case.

6   Were there other-use cases or other aspects

7 of this that you all might have that we can think about

8 beyond these items here, or do you have some feedback?

9 Maybe some of these things aren't important as -- to

10 worry about that. So we thought we'd ask, open it up

11 and try to stimulate a little discussion on this topic,

12 on this end if folks have thoughts. Yes, Suzanne. Can

13 we get the microphone back? Thanks.

14   MS. SEARS: Suzanne Sears, University of

15 North Texas. Chain of custody is important to us. And

16 it being in the meta data would be fine with us as

17 well. But it is definitely something that we want to

18 see with the document.

19   MR. HANNAN: Yes. Harold?

20   MR. BOOTH: Harold -- I think I can probably

21 streamline [inaudible]. Someone did say that the chain

22 of custody is important to them, and you said -- the

1 reason why I wanted to speak up is you said meta data.

2 By that, do you mean that you just wanted to know that

3 it went from one person, to the next, to the next and

4 just I'm asserting that, I'm attesting that? Or do you

5 want a non-repeat -- such that I've signed it, I hand

6 it to somebody else, they sign it, and then I hand it

7 to somebody else and they sign it?

8   It's very different than just putting meta

9 document into the document and saying it went from this

10 person to this person, to saying I've signed it, and

11 someone else signs it, and then party C signs it, and

12 no one can say, I never signed it. So I just wanted to

13 make sure that you understand that there is different

14 technologies that come into play depending on which way

15 you want to go.

16   MR. HANNAN: That's a very interesting point.

17 And so, yeah, how do people feel about that?

18   MR. DAVIS: Ric Davis, GPO. I can tell you,

19 from a policy standpoint, the easy answer is we want it

20 all. Because associated with authentication, you know,

21 we want confidentiality, authenticity, integrity, non-

22 repudiation, all four elements.

1   MR. BOOTH: Right.

2   MR. HANNAN: And so that starts to drive you

3 into the digital signature, only because it is harder

4 to deny a part in the process, if you will, not that

5 folks want to do that, but again, pros and cons.

6 There's not really a right answer. Selene?

7   MS. DALECKY: Selene Dalecky, GPO. Where

8 this also gets a little tricky and comes into play is

9 earlier when we were talking about from a signing, you

10 know, affixing a digital signature to a government

11 publication that we need to distribute, does it go to -

12 - you know, are there a hundred signers from an agency

13 that's a person's name who is signing this document

14 that's going to the public, or is it a role, like

15 superintendent of documents?

16   Or is it, you know, one person who is --

17 assumes the authority of signing, but really, it's just

18 kind of in name only, and what happens when that person

19 leaves? Does it -- you know, does the weight of the

20 signature get carried with you indefinitely because you

21 affixed it to a publication that's now into the public?

22 So from a non-repudiation standpoint, is that really

129

1 important in distributing the electronic government

2 documents, or is that, again, a little bit of an

3 overkill?

4   And then in what cases is it important? I

5 mean, I'm sure that when we look at, actually, the

6 first receipt of the content into FDsys, for example,

7 from agency customers, that would be the point where we

8 would want to know that the person who has the

9 authority to give us the final version of this document

10 for distribution has signed off on it, be it the

11 printing officer or whoever it's assigned to.

12   I know that's the case over with the Office

13 of the Federal Register with their eDOCS system.

14 Agencies are now sending their public -- their notices

15 and their articles that go into the Federal Register to

16 OFR by email that's been signed so that they have that

17 non-repudiation. In that case, it's important.

18   So I think the strong distinction of where in

19 the chain of custody those various levels are needed is

20 important.

21   MR. HANNAN: Yeah, I think -- this is John

22 Hannan, just to add a little bit because this is a

1 nuanced point that most of you folks probably haven't

2 really been thinking about too much, or maybe you have,

3 but just hopefully to be helpful.

4   It is interesting about the concept of a

5 person's name versus the role that they fulfill at an

6 agency, especially with respect to perpetuity and

7 preservation. And there are different ways of coming

8 at this. When you have an individual signing a paper

9 contract or paper agreement, often times, it's not only

10 their name but their role showing they have the

11 authority to bind the agency or the organization to

12 this agreement that's being fulfilled.

13   So -- and you can kind of see how we can come

14 at it at the GPO already in terms of it's not a

15 person's name, it's the role of the superintendent of

16 documents, because that's such a longstanding

17 identified rule. So that's something that is important

18 to think about a little bit as a community as we go

19 through this, and there are pros and cons both ways.

20   Some of the drivers that would say, looking

21 at role-based certificates, which require, you know,

22 again, more handling that goes around them at the

1 beginning before they're substantiated, it can have

2 some payoff down the road, as opposed to 30 years later

3 looking at something and saying, oh, you know, John

4 Hannan signed something. Which if, as long as there's

5 a lot of binding of my title in my personal

6 certificate, that can be -- that can overcome that.

7   But oftentimes, you don't want to churn

8 through if I change, you know, jobs within an

9 organization, or have to churn through different

10 certificates, so just interesting. I thought maybe

11 that would be helpful to you, so probably you have --

12   MR. YU: Yeah, I was hoping to step back just

13 a little bit. I don't feel like I have a good sense of

14 the current state of government's [inaudible] -- so

15 who's the master signer, or who's the central trust

16 authority, and -- who currently has keys, who has

17 ability to sign? How is that sort of managed? I don't

18 really have --

19   MR. HANNAN: Well, that's a great question,

20 and I have all that information if you'd like to know.

21 So -- and you probably might not be surprised at the

22 end, Harlan, that there is no central authority for the

1 U.S. Government because nobody could agree on giving --

2 seeing that to someone. So what it is is it's a hub,

3 it's a hub and -- where there's the federal bridge

4 certification authority, which is essentially a hub, to

5 allow other issuers to meet a common set of policy and

6 procedural requirements, and that's how it's been

7 substantiated at the Federal Government, thanks to NIST

8 largely taking a leadership role in that many years

9 ago.

10   So that's how it's substantiated today.

11 That's been borne out mostly through the HSPD-12 PIV

12 card programs within the Federal Government Executive

13 Branch side, which is like an initiative that the

14 Federal Government undertook several years ago to

15 provide a standard form of ID card. It also had

16 digital certificates on it as well setting up the

17 potential to be used for various topics like this sort

18 of supply chain orientation potentially.

19   And there are -- some agencies issue their

20 own from their own PKI. Some do choose to use a

21 provider that GSA, on behalf of the federal PKI,

22 certifies and is linked into that hub. So that's kind

1 of the high-level answer to your question.

2   MR. YU: Is there a lot of document -- I'm

3 sure there's a lot of documentation. Is it possible to

4 sort of --

5   MR. HANNAN: Yes.

6   MR. YU: -- send it around or put it up

7 somewhere where I could find it?

8   MR. HANNAN: Yeah, sure. I'll give it to you

9 offline because there's a lot of links that I can give

10 you. And we do, also at GPO, have our own public key

11 infrastructure. We're one of two federal agencies that

12 are authorized to issue to other agencies. Treasury

13 Department is the other one.

14   So we've gone through all those processes

15 which are not trivial to be able to issue digital

16 certificates, which is one of the reasons that the

17 agency undertook this several years ago was to position

18 ourselves to be ahead of the curve for suppliers at the

19 agencies if we want to start to take more steps with

20 this, but it's also, you know, our requirements are

21 much like -- I think Ric mentioned, or Selene actually

22 mentioned with the Federal Register, which our

1 viewpoints are looking for issuers that are cross-

2 certified to the federal PKI.

3   MR. YU: Thanks.

4   MR. DAVIS: Ric Davis, GPO. As John

5 mentioned early on, you know, we are cross-certified

6 with the federal branch. I think if you go to that

7 website, there is a link to our certificate authority

8 statement, at least right off of there as well.

9   MR. HANNAN: Great question. Anything else?

10 Yes, Jonathan?

11   MR. MAYER: I guess I'd like to do a little

12 probing on what exactly the threat model is in these

13 chain-of-custody cases. I mean, certainly [inaudible]

14 and if there are kind of external considerations,

15 whether it's good policy or so on, certainly.

16   But in terms of threat model, I guess, the

17 vulnerabilities I see are either there is not an actual

18 signature before something got to the GPO, and that

19 somehow kind of slipped through the cracks, or the

20 GPO's key was somehow compromised or the algorhythm

21 they're using to sign was broken, or someone got

22 really, really lucky, like in the cryptological sense

1 of lucky. So, I guess, from a pure security

2 standpoint, I'm finding it hard to see how it adds that

3 much, if the GPOs already have this terminal signature.

4   MR. HANNAN: I think that's a great question.

5 That's one of the things we want to try to get some

6 feedback on here is, you know, again, in an ideal

7 world, if adding strong signatures for chain of custody

8 cost zero and was easy to do, of course, you would do

9 it. Well, the reality is it doesn't cost zero, and it

10 may or may not be easy to do.

11   It will be easy to do based on the decisions

12 that we end up making, as easy as it can be, but that

13 is, actually, the fundamental root of some of the

14 things that we're struggling with is how best to

15 provide this, at least initially, so that it's on a

16 strong note. But you kind of, I think, really

17 crystallized it, Jonathan, so thanks, that's -- that's

18 a good one.

19   So do others have thoughts about that, like

20 oh, you know, I think Suzanne's already commented on

21 this, and I think that?s great, is that, you know,

22 chain of custody is good enough, and Harold, rightly,

1 pointed out some of the other -- the classic on-the-

2 other-hand point of view which is, well, it has its

3 limitations too. So I think that's really what we're

4 looking at at GPO is, you know, what's the sense of

5 people -- is a meta data orientation good enough? Don't

6 worry about it for now, look at bringing in other stuff

7 down the road.

8   And in that regard, if we start off with meta

9 data that proves not to be good enough, are we really

10 fined. So Suzanne, you have -- thanks, Ted.

11   MS. SEARS: Suzanne Sears, University of

12 North Texas. Going back to what -- going back to what

13 John said earlier, 80 percent of my users, you know,

14 they're going to trust that what's in the library is

15 valid, and they're not going to care about chain of

16 custody. For me, it's important --

17   MR. HANNAN: Sorry about that. It's --

18   MS. SEARS: I'll just talk loud. For me,

19 it's just really, really important to know that it is

20 an official agency publication and not just something

21 that John Smith who used to work at, say, the OTA and

22 it's an OTA document, but his own version of this

1 document. So for me, the meta data is okay, but I'm not

2 a technical person, I'm just the end user who doesn't

3 understand anything that you said. So --

4   MR. HANNAN: That's okay.

5   MS. SEARS: I mean, I know my catalog record,

6 which I'm sure you could not mark catalog, but I know

7 which field it goes in my mark catalog record, and when

8 I'm creating meta data for our digital collections,

9 they're based off those catalog records.

10   And for us to just know that, you know, this

11 is an official publication from the Department of

12 Energy, or this is an official publication from the

13 Government Printing Office, that's the important part

14 that I need to know. So the tech part behind that, I

15 can't really give you comments on that.

16   I can just tell you as an end user, we do

17 need to know that it is an official publication. And

18 in the printed form, we have that because it says,

19 printed by the Government Printing Office.

20   MR. HANNAN: That's great. That's super

21 helpful. Thank you. I think that's absolutely

22 important. Mary Alice?

 1   MS. BAISH: I think a distinction needs to be

 2 made with what the role of the GPO is in the digital

 3 world when we're talking about chain of custody. For

 4 example, speaking of the courts, it is the judge or the

 5 reporter that verifies, whatever term you want to use,

 6 what is going to become the official version, say the

 7 Court Opinion, and so much of that chain of custody is

 8 going to happen at the publishing agency or the senate

 9 or the congress or the individual court, not at GPO,

10 because you're not that official publisher.

11   So then it's -- at what point in that chain

12 of custody do you all have a role in kicking in and

13 tracking it so that you can then be that third party

14 authenticator?

15   MR. HANNAN: Thank you. That's, I think, a

16 really great way to personalize it in many respects.

17 Others, before we move on from the chain of custody

18 topic? Hearing silence -- oh, Harold.

19   MR. BOOTH: Sorry.

20   MR. HANNAN: That's okay. No, it's great.

21   MR. BOOTH: She mentioned that you know that

22 it's been printed by the Government Printing Office, so

1 putting on -- I'm about as paranoid, I think, as Kevin

2 over there. How do you know that it was printed by the

3 Government Printing Office? I could just stand up my

4 own printing press and print off anything I want.

5 That's issue number one.

6   Issue number two, I think one of the things

7 that's kind of left unsaid a little bit here is that

8 when we're talking about digital documents, publishing,

9 you know, myriads of multiple different types of

10 versions of copies is, actually, relatively cheap and

11 inexpensive relative to how it used to be where I had

12 to get a printing press and, you know, a binding book

13 and do all this stuff. It was a huge investment in

14 money, so only large organizations could do it.

15   Whereas now, anyone with a computer could

16 just basically publish something and, you know, they

17 could make it look like a formatted GPO document and

18 then send it off to the world and instantly have, you

19 know, literally millions of copies floating around.

20   MR. HANNAN: Well, I think that's why we're

21 having this workshop.

22   MR. BOOTH: Right, well, I'm --

140

1   MR. HANNAN: But you're right. You hit it

2 right on the head in terms of -- and again, one size

3 fits all? Maybe it isn't -- you know, we're trying to

4 figure it out, I think, as an integrated community. So

5 -- yes, Steve?

6   MR. ANDERSON: The more I think about this

7 the more I think that it's really an important -- a

8 more important discussion to have than I had originally

9 envisioned, simply because on the one hand, and looking

10 at this through, you know, both the history of the book

11 as well as, you know, what other state agencies' needs

12 are if anything's ever going to be replicated, one of

13 the things is that the chain of custody, essentially,

14 between the first -- between saving the document on

15 somebody's PC and having it be "printed or published by

16 GPO" is probably a much more cumbersome and convoluted

17 process than we think.

18   It goes through editorial processes or

19 whatever. At what point in time does everybody feel

20 comfortable saying we, you guys, are going to sign off

21 on this document at this point in time? And you're

22 right about threat models and, you know, what's the

141

1 risk. And, you know, quite frankly, we could probably

2 afford a little room to be flexible.

3   But realistically, we need to do two things.

4 One is making sure that we have this stuff locked down

5 so that posterity and judges and legislators are going

6 to say this is the official thing and has been for the

7 past 70 years. That's number one. Number two is you

8 want to still incentivize very much the creation of

9 digital media. And it is not like the print world in

10 that way. I mean, you're right.

11   Anybody with, you know, a Blackberry can go

12 ahead and publish whatever they want, essentially. And,

13 you know, that's a very different model, and we want to

14 still incentivize people to produce content and not

15 necessarily lock them down into some type of very

16 regimented process, but you want to -- you want to, at

17 the same time, leverage that ability to produce

18 information, but at the same time, provide a

19 significant assurance that, at some point in time, it's

20 right.

21   So my suggestion would be if there's any way

22 to kind of punt that whole issue somehow to some type

142

1 of working committee for further public input might be

2 beneficial where transparency or -- I don't -- I think

3 there's room to be a little more exploratory there.

4   MR. HANNAN: Thank you. That's great input,

5 I think. Yes, sir.

6   MR. SHULER: John Shuler, University of

7 Illinois, Chicago. Spinning off of that, I think the

8 great advantage the GPO has over any other agency is

9 what I call nested authenticity. You not only have

10 technical tools, such as chain of custody, PGI,

11 whatever; you also have associated with you socially

12 and politically, economically, a set of depository

13 libraries that provide another level of authentication

14 in a social setting.

15   And your relationship with the other

16 agencies, the dealings that you have with them

17 exchanging, for instance, the Federal Register, is a

18 further form of authentication.

19   I think where you spin off the idea of the

20 further working group, if you move it from just a

21 technological solution to -- more into Ric's world, the

22 policy solution, it's going to become multifaceted, and

1 I think you move away from that conundrum that

2 everything has to be solved one way, every chain of

3 custody problem has to be solved with the same tool.

4   But I think what you're experiencing in this

5 room a little bit is we have a multiple chain of

6 custody issues that can be solved in different ways,

7 and not all of us have to be resolved by what would be

8 a strict, orthodox, legalistic point of view of what

9 chain of custody is.

10   MS. DALECKY: Selene Dalecky from GPO. Just

11 to kind of piggyback on that conversation and what was

12 going on with Suzanne and Harold in the discussion of

13 how do you know it was printed from GPO, and I think

14 one of the things that you can refer back to is kind of

15 what John just said where Suzanne really put herself

16 into the chain of custody, if you will, by being a

17 depository library, by receiving the printed book from

18 GPO directly or from a trusted source with the inter-

19 library loan or in some way like that and, therefore,

20 can vouch for the authenticity of this particular

21 publication in hard copy.

22   And then the same could, I think, be modeled

1 in the electronic world where how do you know this file

2 -- as Suzanne points a patron to an electronic version

3 of a document, well, it was retrieved from a repository

4 maintained by GPO, and we have the same assurance from

5 the originator and from the system that it was

6 maintained in that this is reliable.

7   If you extend that even further out, when we

8 talk about system-to-system content and how can we be

9 assured that from system -- system B has content from

10 system A that's the same and can be assured. If you've

11 got that type of trust between the two systems in, say,

12 an approved -- an approved depository repository where

13 the transmission of the content has been assured and

14 the maintenance is assured at the depository end, you

15 again can have assurance of that particular data set.

16 So I think it can keep extending and follow and model

17 the print world, at least through that process.

18   MR. SHULER: Another way to look at it, the

19 chain of custody is not protecting the document itself,

20 although it's a vital part of it; it's protecting the

21 relationship that the document establishes. And on a

22 very legal -- that relationship is extremely tied

145

1 together to that particular document. But in

2 relationships fostered by GPO through its

3 multiplicities, that authenticity can take place in

4 different ways in congruences rather than in specific

5 non-overlapping applications, if you will.

6   MR. HORTON: This is Bob Horton from the

7 Minnesota Historical Site. Is that another way of kind

8 of saying you're developing a routine?

9   MR. SHULER: Yes.

10   MR. HORTON: Yeah. And then the routine

11 course of business is a legal term and does have

12 evidentiary value. And maybe that's why we're kind of

13 struggling with this because no one has developed a

14 routine. You are inventing a lot of these things. And

15 with the recognition that the technology will change,

16 you'll have to reinvent, but the routine is the goal.

17   And you can -- maybe there's a way of

18 prioritizing this. Some of these routines will be

19 easier to establish than others, and that's probably

20 the place to focus, I guess. But I think you guys are

21 right on target with that approach.

22   MR. MAYER: I guess I just briefly want to

1 flag from a technical perspective this idea that

2 decentralized authentication, if you will, working with

3 depository libraries and so on, this has been tried

4 before in other computer security contexts. The one

5 that comes to mind is authenticated websites, making

6 sure that they are actually who they say they are by

7 kind of using almost certificate depositories

8 throughout the web.

9   It's proven to be pretty difficult getting

10 everything synced up, a lot of problems getting

11 adoption, users tend not to want to check against a

12 bunch of different certificates, especially if it

13 requires a lot of network access. Some folks might

14 just want to use offline validation. So from other

15 contexts, at least, I do want to flag that this has not

16 been the most successful approach.

17   MR. HANNAN: Okay. Other viewpoints or

18 thoughts? This has all been really helpful. If not,

19 let's try moving to this next one because this is very

20 quick, I think. Re-authentication over time, this is

21 really more just to make -- provide some awareness for

22 you about what can -- I think Kevin brought this up

1 earlier today about the fact that you may need to re-

2 authenticate content based on events that would occur.

3 Challenge number one, algorhythms and techniques change

4 over time -- start talking ten years, and sometimes

5 it's five years or less, potentially. And some examples

6 of that are shown on your handout.

7   Challenge number two is the thing that keeps

8 the computer security people up at night sometimes and

9 that is sort of issue with the mathematics involved,

10 that ends up meaning that quick action needs to be

11 taken. So this is just a challenge for us. Not so

12 much -- we just wanted to give you a little bit of

13 awareness that we are thinking about this.

14   So our current planning is maintaining

15 awareness about the requirements of the changing nature

16 of authentication standards. We are continuously --

17 Selene and myself [inaudible]. Periodically assessing

18 the requirements of re-authenticating content more

19 frequently than annually, if we need to. We kind of

20 look at that at least once a year.

21   We need to start, plan to start re-

22 authentication along [inaudible] requirement changes,

1 rehab of automotive [inaudible] authentication

2 [inaudible] utilize, fortunately, for that, but it

3 still provides some challenges to the problem.

4   Lastly, what we plan to do with the industry

5 data we mentioned is to canvas industry and suppliers

6 of technical systems for innovative solutions that they

7 may have which would take advantage of -- take

8 advantage to help us in this regard.

9   Hard problem, especially based on just the

10 size of the repository. If you thought you wanted to

11 re-authenticate that, in a short period of time, that

12 gets more challenging than if you want to do it well

13 ahead of when you think you might be wanting to do

14 this.

15   So this is our plan, and hopefully, we'll

16 have some interesting things that come out of the

17 industry that we can communicate, innovative solutions

18 for this.

19   At this point, I think we're at a decision

20 point. This is our last topic for today. We can

21 either take a short break and come back, or just plow

22 right through it and get done. Most people say plow

1 through it and get done. Is that what folks want to do

2 for the most part? That sounds good.

3   So with that in mind, I want to make sure we

4 give you a choice. The problem statement for us, it's

5 been a challenge. You know, what is granular

6 authentication? It's not easy to say, obviously,

7 either for me. So the way that we tried to formulate

8 this was from a couple of points of view. One, to

9 authenticate an arbitrary portion of the document.

10   One page out of 500 were sent in. And the

11 other perspective is locating, you know, tasks and

12 relating it to a GPO authentic document. Maybe that's

13 a useful thing, with the goal being, you know, getting

14 an authenticated answer in a reasonable amount of time.

15   As we thought about this, and I'm going to go

16 to a concept we have in the next slide just to get your

17 feedback on it, the concept of trying to pre-

18 authenticate, you know, sub-slices of content almost

19 seems like a fool's errand to some of us. But, you

20 know, it kind of cuts both ways because as soon as you

21 spend all that time pre-authenticating things, it's

22 really not useful to the next person that comes into

1 queue for how they want to slice down out of a 500-page

2 document they're interested in.

3   So we have a concept on the next slide. It

4 really goes to the second point above, which is this

5 concept that you're trying to -- you have some text,

6 and you really think it relates to some document, but

7 you'd like to be able to have a definitive link back to

8 the authenticated publication for GPO.

9   So let's just step through this real quick.

10 I know it's probably hard to read. It's probably hard

11 to read in your handout. I apologize. We can try to -

12 - when we post this on the website later -- increase

13 the font so it's not too much of an eye chart.

14   But this concept is just a concept. Nothing -

15 - we just wanted to get your feedback to see if it was

16 useful or not. The first step is a user's got some

17 information they think -- that they have, but they're

18 curious if it's really what the statute says, let's

19 say. There may be bad examples. But not quite sure

20 which one it was.

21   So the second step is that they would ask our

22 system, I've got this text, I think it comes from a

1 statute. Can you help me? Our system would provide

2 back a box on the screen that says, go ahead and answer

3 the text. If you think you know something about the

4 document that this is from, enter that too.

5   Then our system, in step four, will try to do

6 a search through our authenticated material, may

7 provide more than one hit and give you a sense of if

8 there is more than one hit. And in step five, the user

9 can say, oh, that. I thought that that was the statute

10 it came out of. Great. Click on that and we could,

11 potentially, provide a signed and real-time statement

12 that this text is in this file. Does that sound like

13 it would be something if we could do that that would be

14 useful?

15   MR. SCHWEICKHARDT: John, Reynold

16 Schweickhardt. Let me just add one of the concepts

17 here is also from a burgeoning and effectivity point of

18 view, so if you simply search for text and you find it

19 in a repealed statute or appropriations bill from four

20 years ago instead of current law, you haven't found --

21 haven't found the hit you were looking for, we're

22 thinking that part of the value-add here would be able

152

1 to talk about burgeoning and effectivity of the hits

2 that potentially would come back.

3   MR. HANNAN: I mean, clearly, this is a

4 little bit like orienting a Google search. If you do a

5 Google search on one word, you might get 10 million

6 hits. If you orient the Google search -- or any kind

7 of search, a little more carefully, a more reasonable

8 answer can come back within a reasonable amount of

9 time.

10   So there's a lot of that kind of aspect that

11 we play into this, but this was something that a lot of

12 us here have just kind of kicked around thinking, you

13 know, if we had a capability to do something like this,

14 would it be of value?

15   It kind of felt to us like it might be of

16 value to people in your arena, so I think we might

17 could just see if that makes sense. And if it does,

18 then maybe we can look at what's involved in that,

19 which it could be really hard, and you can end up doing

20 it.

21   MS. BAISH: I think it's a very exciting

22 concept. And in previous discussions, I know Mike and

1 Selene when we talked about the granularity, this is

2 not the kind of value add delivering back to the

3 customer that I thought you were talking about. The

4 limitation I see is it's only going -- would only apply

5 to the content of FDsys.

6   But it also, what it gets to is the issue

7 when a user goes into a court opinion on Google Scholar

8 or on West or Lexis, that they could take that granular

9 piece up against, hopefully, what is in content of

10 FDsys and verify it with your authenticated version. So

11 from that component, I mean it's really kind of an

12 exciting idea.

13   The limitations being it's your content only,

14 but it gets back to one of my earlier comments that in

15 the ideal world, someone could look at electronic court

16 opinion and be able to find out whether it's I a

17 commercial database or on a website or on GPO and third

18 party be able to check the authentication. So this is

19 great. I hope there are ways for you to do it,

20 actually, or explore that further.

21   MR. HANNAN: Great. Thank you very much.

22 That's what we were looking to see. Yes?

1   MS. CASE: Are you thinking that you'd only

2 go for an exact match?

3   MR. HANNAN: I think we would have to --

4 fuzzy logic kind of principles, get too tricky. This

5 is probably going to be hard enough. It would have to

6 be spaces. It probably would have to be an exact

7 match, exactly.

8   MS. CASE: So any system that repurposed the

9 data and took out some text in the middle, your search

10 would fail.

11   MR. HANNAN: In this concept because we're

12 not trying to evaluate somebody else who's got the

13 legitimate thing, we're trying to do what we can.

14   MS. CASE: So it would be an exact match.

15   MR. HANNAN: Yeah.

16   MR. WALSH: And this is just one scenario,

17 right? It's one thing considered as an option. There

18 are others that you would explore.

19   MR. HANNAN: Based on, yeah, what --

20   MR. DAVIS: Ric David, GPO. Another point to

21 add to this issue, you note in the example John

22 referenced one page as an example, which would be hard

1 enough. I can tell you that in some of the use case

2 discussions that we've had, people have said why limit

3 it to one page? Why not make it a paragraph, a

4 sentence, a word? And the thing to consider in all of

5 that is context.

6   You need to be able to map it back to the

7 original document so that the authenticated granular

8 content is considered within the context of the actual

9 document, so that's a consideration. I think that if

10 we could do it with a page, we would go from there, but

11 I think that would be a logical start as opposed to

12 even getting down to a smaller more precise segment of

13 content.

14   MR. HANNAN: Well, I think that's a good

15 point, Ric. This concept here really deals with that

16 second point on the slide before. And in this case,

17 what we're putting more on the user to exactly type in

18 a paragraph they're interested in.

19   If they're willing to do that, I'm willing to

20 wade through all the hits that might come back, and

21 there probably are ways we could help make that a more

22 meaningful display of the hits. This kind of gets it,

1 a kind of general purpose way of thinking about that,

2 but there's a lot -- it's going to end up being a

3 pretty good bid on the user involved in terms of how

4 they structure their search. Yes, sir?

5   MR. MAYER: So I guess my reaction to the

6 proposal is it looks a lot like search to me.

7   MR. HANNAN: Well, yeah.

8   MR. MAYER: I guess you could look for an

9 exact match, you could kind of do a little bit more

10 fuzziness. And then the crypto piece at the end, I

11 guess, you could certainly, on the fly, sign specific

12 elephants.

13   You could also run this entire thing over

14 https, you get the same security guarantees. The only

15 difference is it's kind of not portable, you can't take

16 that signature away with you. So if that's -- fair

17 enough. But beyond that, I guess my reaction is it's

18 search.

19   MR. HANNAN: Thanks, that's good.

20   MS. CASE: It's also search on a large

21 segment of text, and it's tough to get a -- well, first

22 of all, most full-text search engines don't do exact

1 matches well. It's going to be a tough search to

2 build.

3   MR. HANNAN: It might be. I think that's why

4 we wanted to see, first of all, if it was possible and

5 -- is it of value? That's really the question we'd

6 like to get some feedback from you on. We can work

7 through some of the practicalities. We don't know that

8 this is really feasible at all as a concept to gain

9 some feedback from -- if it was feasible to do, would

10 it be of use? Because if you said no, it wasn't any

11 use, I wouldn't go any further with it. But that's a

12 great point.

13   You're absolutely right, and thank you for

14 bringing it up. You're right. It's a hard problem.

15 Just about like every topic we've talked about today is

16 a hard problem, and that's why it hasn't been done yet.

17 Yeah? You have it, Jessica.

18   MS. MCGILVRAY: I think that there definitely

19 is value here. And it reminds me of what they're doing

20 with electronic management -- electronic record

21 management at NARA. They're creating a search field

22 and working. So if you do decide to go to this, that

1 might be something -- I don't know.

2   MR. HANNAN: We might be able to collaborate.

3   MS. MCGILVRAY: Yeah.

4   MR. HANNAN: Oh, that's good. Thanks. Yes,

5 sir?

6   MR. ANDERSON: I agree with Pat in terms of

7 the caution about scalability. And I agree. I think a

8 lot of the execution of this -- I mean, number one, I

9 think it's pretty cool. But number two, I mean, given

10 whatever resources that you might need to bring to bear

11 on this, I mean I think off the top of my head, there's

12 a scalability issue because you might have an

13 expectation to find the sentence. And that is going to

14 be very tough to do, I would think.

15   The second thing is that this presupposes

16 that the end user is already using not an authenticated

17 version, it would seem to me. Somebody's getting, you

18 know, an unauthenticated copy of the Federal Register

19 from Lexis or West Law, and then they want to make sure

20 that that's the real deal.

21   So it's kind of -- if you've already created

22 it before, I mean, I guess my question is -- I mean,

159

1 obviously, there's that scalability issue going the

2 other way. If you're going through the entire issue of

3 the Federal Register, you do want to find what it is

4 you're looking for. But, you know, why aren't you

5 using the original thing to begin with?

6   MR. HANNAN: Well, I think that's an

7 interesting question. Let me give you my take on it,

8 which is this actually does support that use case,

9 which is I've got the 500-page document, and I'd like

10 something signed on this paragraph. I've got to type

11 in the paragraph, or cut and paste it. Then you can

12 get an actual signed granting of that at your arbitrary

13 convenience, even though you've got the 500-page

14 authenticated thing.

15   Now I don't know if that's a bit of use.

16 That was kind of the concept here is you actually could

17 do - - even if you already had the authenticated

18 piece, you could supply the file name which would make

19 this search probably very scalable.

20   MR. ANDERSON: Right.

21   MR. HANNAN: It's GPO's site -- to figure out

22 --

 1   MR. ANDERSON: And what's the end result to

 2 the user?

 3   MR. HANNAN: We don't know yet except it

 4 would be a signed data structure in some format that

 5 you could, you know, PDF -- probably PDF is the most,

 6 honestly, practical thing for us to do given the

 7 challenges with signed XML. It would probably be a

 8 signed PDF of that saying this exact text is found in

 9 this file, maybe the URL. I mean, we haven't really

10 gone very far with this.

11   We really wanted to just kind of preview it,

12 see if it sounded like it would be of value, and we

13 could start to go back and sharpen our pencils a little

14 bit and see if it's something that might actually show

15 some progress here. So -- I mean, those are the kind

16 of things, really, we're thinking about.

17   This text -- all we can assert is, oh yeah,

18 that text is in this document, and we would be willing

19 to do that, I think, although I always have to talk

20 more to lawyers, honestly, if it's valuable.

21   MR. ANDERSON: I mean, we can quickly,

22 following up on that comment, I mean one of the things

1 that somebody is going to have to do in the legal world

2 anyway is to see what the context of the quotation is

3 anyhow. So the second -- the other user down the road

4 from the information provider, who is user number one,

5 is going to have to synthesize whatever snippet,

6 whatever official snippet that is by going back to the

7 original document anyway and taking a look at the

8 context in which that's located, I would think.

9   MR. HANNAN: Well, I think, you know, that's

10 a good point. So, having thought through this a little

11 bit, the better you structure the signed thing you get

12 back, probably the easier the interaction between user

13 one and two is. With regard to that, certainly, the

14 goal here is to -- the user two in your concept, where

15 user one gets this signed data structure, you know, if

16 user two wants to go back to the official source, they

17 can clearly do that. That's great.

18   And maybe over time, that data structure will

19 obviate the need for time to be spent by users two,

20 three and four, potentially, maybe if it's -- so that

21 would be the -- that's the thought process about why

22 this might be a useful thing to, you know, put some GPO

162

1 resources towards perhaps -- we just really wanted to

2 get -- does that make sense to you?

3   MR. ANDERSON: Yeah.

4   MR. HANNAN: So we wanted to really get some

5 feedback from you all about did it sound like something

6 that might be worth looking into. It sounds like,

7 generally, it might be. Yes, sir?

8   MR. MAYER: This occurred to me earlier.

9 Yeah, I think there actually also could be some really

10 serious security concerns doing this. If someone can

11 submit something, let's say comments to an agency or

12 something like that that gets published by the GPO and

13 you're willing to sign it, then you've kind of given

14 away the ability to arbitrarily sign anything with the

15 GPO key, which could be bad. So let's suppose --

16   MR. HANNAN: I'm sorry, yeah, could you

17 explain that?

18   MR. MAYER: So the idea being, let's suppose

19 some bad guy wants to get something signed with the GPO

20 key. As long as they could get it into any document if

21 you're willing to sign at any level of granularity,

22 they just say sign that passage, that will --

163

 1   MR. HANNAN: Didn't we already put that into

 2 a file that's signed and published on the Internet?

 3   MR. MAYER: So you're signing the entire file

 4 instead of just the little snippet. And so the idea

 5 would be, you could imagine a tax where they want just

 6 a snippet signed. Because that can be bad, for

 7 example, if you're using a key.

 8   MR. HANNAN: Right. So this --

 9   MR. MAYER: Something to think about.

10   MR. HANNAN: It is. That's a great point,

11 Jonathan. I really appreciate it. This gets down to

12 what -- okay, so this just says that you made a comment

13 in a document that was published. That's what would

14 come out of that signed data structure. And so it does

15 speak a little bit to, you know, that's all it would

16 say, you know, to the person that you would show this

17 to. And so, again, it gets back to the context that

18 Rick mentioned, and that is an interesting -- we're

19 trying to sort through that to about, it really

20 dovetails with Steven's comment about it's easy to like

21 -- it's easy to find the word "the" in all kinds of

22 documents. That's not --

164

1   MR. ANDERSON: Or it's hard.

2   MR. HANNAN: Well, yeah, right. It's

3 certainly not very useful.

4   MR. ANDERSON: Yeah.

5   MR. HANNAN: Yeah, it's not -- so you raise a

6 good point about what can you really say. And that's

7 why the wording about all this says is this text is in

8 this file. It doesn't say anything more than that. And

9 that may or may not be as useful. Certainly, if it's a

10 big long string of text with a lot of context to it and

11 a file that's pretty definitive and descriptive in its

12 name, then you can start to use this more, you know, as

13 human beings for useful business or whatever.

14   So that's all I -- I think it's a good point,

15 and it's again, I think we'd have to think through this

16 too so that we provided something that was really

17 useful and wasn't subject to being misused. You're

18 absolutely right about that. So we have to be really

19 careful about, you know, the little asterisks on the

20 fine print and what came out of this. So I appreciate

21 you saying this. Thanks. Harold?

22   MR. BOOTH: So, just to kind of add on to, I

1 think, some of the various comments from what I heard,

2 basically, perhaps just turning back, you have

3 everything already up on the web, turning back a URL

4 that provides what -- it sounds like people like the

5 search capability. So you provide the search

6 capability, and the response could be, you know, here's

7 the URL, and the fragment of the document from which

8 that particular text was found, or fragments where it

9 was found.

10   And that fragment or URL can be shared

11 amongst people, and people can then go to GPO

12 themselves and then go and get that source document.

13 But they get to go right to the location or citation

14 that's of interest to whoever originally got that

15 particular fragment or piece of document.

16   MR. HANNAN: Right, I think that's kind of

17 what we had in the back of our minds here.

18   MR. BOOTH: The point being is you wouldn't

19 need to have a signature over everything. You'd just

20 provide a URL. They always have to come back to GPO

21 servers to get that information.

22   MR. HANNAN: Well, I think that's the --

1 that's an interesting point about this concept is

2 because you're trying to get out of a 500-page file

3 that you're carrying around and showing to somebody.

4 And so it's tricky, everything that's been pointed out,

5 it's kind of tricky to think about how to bring value

6 in that regard, but I think your comments are right

7 along and good.

8   So this is helpful to us to think about,

9 again, it's all predicated -- and as Steven and Pat

10 pointed out -- it's really predicated on being able to

11 get an answer back in a reasonable timeframe. And

12 that's going to take some work on our part to think

13 about and see if that's really achievable. There might

14 be some limits on, you know, it's not just a sentence.

15 It's maybe a paragraph at the smallest segment,

16 something like that. So we have to think about that

17 too. Yes, Steve?

18   MR. ANDERSON: Well, it also is going to

19 depend a bit on the historic development of what a

20 piece of information content is going to look like,

21 what the package itself is. Because my hunch is that

22 at the same time, you're going to have more 500-page

1 documents coming. You also might have a lot fewer 500-

2 page documents coming, and you're looking at

3 information content being sentence-by-sentence or

4 paragraph-by-paragraph anyway, and looking at

5 granularity in terms of authenticating individual

6 content packages that are tiny rather than very, very

7 large.

8   So, you know, I guess what I'm saying is we

9 could go both ways from here on out. I mean, you might

10 have a lot more volume in your file to authenticate.

11 But you also might have a lot fewer pieces and it

12 really goes to what approach information design is

13 going to be like, you know, in the next 20 years, or

14 longer.

15   MR. HANNAN: That's a good point.

16   MR. GALLUCCHIO: I think what we're talking

17 about, there's a good argument for your guys to break

18 up the data into reasonable chunks. I mean, you could,

19 theoretically, sign your whole repository with one key,

20 right? And then the user, to authenticate, would have

21 to download that whole repository, and that doesn't

22 make sense, right? So you could do it by book, you

168

1 could do it in chapter, subsection. You know, it's

2 kind of -- it's up to you. You should try to make it

3 practical. It shouldn't be arbitrary. It shouldn't be

4 an oracle where you can just ask it to sign anything

5 you want. So --

6 MR. HANNAN: Well, yeah. That's not really

7 what that -- you don't get to sign whatever you want.

8 It has to be part of a document that's already been

9 signed. But, yeah, that's a great -- that's a great

10 point. I think we struggled with that a little bit

11 too, you know. Which way do you approach it from? You

12 know, pre-signing all the granules, that's really

13 arbitrary small levels. I think that's tough and time

14 consuming.

15 But I think your points are really good, and

16 comments -- I appreciate it. Other thoughts? Everybody

17 tired? Wish there was more coffee out there? Hearing

18 no more input at this point, I think we'll go to the

19 next couple slides, which is wrapping up.

20 And the first thing on this is thank you so

21 much for your time and your participation. It was

22 really, really good. We really appreciate you taking

1 time out of your busy day to come down to GPO and be

2 here. We're going to post information about the --

3 shop at the URL that we have listed there. We'll have

4 the slides from today, the transcript of what we went

5 over in several days, and then we're going to be

6 working on a summary report to try to summarize things

7 for us that we can always go back to.

8   That's going to take us a while to go through

9 that. But if you have additional comments, this email

10 address is set up to accept them, so please go ahead

11 and send us thoughts. We realize you didn't see these

12 slides before you got here, so if you go home or you're

13 on the airplane and you think there's something,

14 whatever, please feel free to email them in, and we'll

15 factor that into the -- report. Mary Alice?

16   MS. BAISH: I just was curious, have you set

17 a date yet for the industry day?

18   MR. HANNAN: No, we haven't yet. We're

19 thinking probably August, September. We would like to

20 do it sooner rather than later, but we want to

21 assimilate all this good input and put some thought to

22 all the things that folks have said, and that helped us

1 make that better. I think -- we haven't really talked

2 about this in a great level of detail with either Mike

3 or Ric, but I think the thought process is that for

4 industry day, you know, if you all want to come, I

5 think that's probably going to be [inaudible]. Exactly.

6 Yes?

7   MS. DULABAHN: Mike, did you want to talk

8 about the federal agencies group?

9   MR. WASH: Yes. Thank you for the reminder.

10 There's a -- part of the INDIF (ph) initiatives, there

11 was the creation of a Federal Agency Digitization

12 Guidance --

13   MS. DULABAHN: Guidelines Initiative.

14   MR. WASH: Guidelines Initiative that is a

15 group of federal agencies working together with some

16 outside support as advisors, I think, is the way it's

17 structured, right, Beth?

18   MS. DULABAHN: Right.

19   MR. WASH: For Xerox and Kodak and others.

20   MS. DULABAHN: Right. There's an outside

21 advisory board, and we've also engaged consultants.

22   MR. WASH: Right. And that's been something

1 that we have used to help develop a digitization

2 specification for preservation initiatives for

3 retrospective documents. We're in the process of

4 forming a similar type of group for authentication that

5 will be, again, a similar type of organization, but

6 it's a federal agency type of organization. It's just

7 in the formation stages. GPO is going to lead that one

8 with participation with other agencies.

9   But I think it would be really helpful to

10 form an advisory group in a similar way with folks from

11 here, if you are interested, to kind of follow what's

12 going on within this working group of federal agencies

13 on authentication and provide advisory input from time

14 to time. So we should probably just kind of reach out

15 and see who would be interested in working in an

16 advisory role on that sort of thing as we get the

17 working group up and running. Anything to add to that,

18 Beth?

19   MS. DULABAHN: I'd just say the focus of that

20 initiative, initially, had to do with digitization of

21 documents. And I think that's one of the things,

22 looking at the topics that have been discussed to date,

1 like chain of custody and so forth, we talked about, I

2 think, primarily born digital documents, and then we

3 had some reference to the print chain of custody, and I

4 think there's a space in the middle that is the print

5 documents that get digitized and move to digital form.

6   And so what I would see as one of the main

7 topics for discussion of that group, among other

8 things, would be what does it mean to authenticate

9 digitized documents, especially when, for example,

10 we've been asked to redact Social Security Numbers in

11 other documents. I think there are a line of nuances

12 related to digitizing documents that, collectively, the

13 federal agencies need to come to grips with.

14   MR. WASH: Okay. So if there's interest in

15 that, we'll be pulling more information together on the

16 formation of it, but I think -- I would say for now,

17 just be aware that that group will be forming. I think

18 there should be some sort of advisory role, and if

19 you're interested, we could form an advisory group for

20 that group.

21   MR. HANNAN: I think with that, we really

22 appreciate it. Thanks for coming, and we're adjourned.

173

1   (Whereupon, at 2:38 p.m., the Document

2   Authentication Workshop was adjourned.)

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

174

```
 1              CERTIFICATE OF COURT REPORTER

 2

 3      I, NATALIA KORNILOVA, the officer before whom

 4  the foregoing meeting was taken, do hereby certify that

 5  the witness whose testimony appears in the foregoing

 6  meeting was duly sworn; that the testimony was taken by

 7  me in stenotypy and thereafter reduced to typewriting

 8  by me; that said meeting is a true record; that I am

 9  neither counsel for, related to, nor employed by any of

10  parties to the action in which this meeting was taken;

11  and, further, that I am not a relative or employee of

12  any counsel or attorney employed by the parties hereto,

13  nor financially or otherwise interested in the outcome

14  of this action.

15

16

17                      _____

18                      NATALIA KORNILOVA

19                      NOTARY/COURT REPORTER

20               IN AND FOR THE DISTRICT OF COLUMBIA

21

22  My Commission Expires: April 14, 2012
```

1

10 63:15 152:5

10:35 71:15

10:50 71:16

100 39:2

11:45 3:1

110th 22:9

111th 69:10

12 104:4

14 174:22

15 63:16 71:16,22

16 59:14

17 25:6

18 1:12

1813 14:21

2

2.0 74:7,12,17

2:38 173:1

20 100:2 167:13

2004 47:4

2005 12:8

2008 22:6

2010 1:12 94:16,17

2012 174:22

22 71:19

256 28:21

3

30 131:2

4

40 60:1

400 41:16

5

500 149:10 167:1

500-page 150:1 159:9,13 166:2,22

7

70 141:7

732 1:13

8

80 92:14 97:3 99:22 101:4 136:13

9

9:10 1:15

95 12:17

A

a.m 1:15

AALL 59:4 95:1

ABA 96:20

ability 51:6 63:18 106:16 125:12 131:17 141:17 162:14

able 4:20 6:18 14:7 27:17 29:1,4 34:3,17 35:6,9 38:5 40:17 42:3 69:18 97:5 100:18 101:20 102:7,9 106:10,18 118:15,16 133:15 150:7 151:22 153:16,18 155:6 158:2 166:10

absolutely 27:12 113:21 137:21 157:13 164:18

abstract 26:11 68:18 78:7

academia 64:14

accept 83:3 169:10

access 7:17 11:19 13:16 22:7 31:20 32:7 58:17 60:1,17 79:14 94:20 95:6 124:11 146:13

accessible 28:22 74:3

accessing 94:19

accomplished 68:11

achievable 48:12 166:13

achieve 21:18 23:20 25:11

acronym 22:13

across 50:13 54:11

Act 44:17

Acting 12:2 14:14

action 147:10 174:10,14

activities 5:8

actor 71:7

actors 30:11 78:13

actual 134:17 155:8 159:12

actually 9:5 13:5 15:21 22:6 30:22

37:9 41:4 47:7 49:12 58:18 65:3 73:10 83:19 90:21 91:18 95:11 99:12 102:2 111:2,15 129:5 133:21 135:13 139:10 146:6 153:20 159:8,16 160:14 162:9

add 12:7 37:8,15 43:13 54:2 62:1 66:7 68:7 70:21 75:10,19 76:14 84:11 87:5 91:13 116:3,13 120:3 122:12 123:4 129:22 151:16 153:2 154:21 164:22 171:17

added 63:3 107:14

adding 40:22 45:4 135:7

addition 106:5

additional 13:18 14:9 30:12 91:21 169:9

address 30:9 103:5 169:10

addressing 13:14

adds 135:2

adjourned 172:22 173:2

administration 15:13

Adobe 5:13 108:4

adoption 146:11

advantage 46:15

54:7 142:8 148:7,8

advantages 109:9 111:2 119:15

advisors 170:16

advisory 170:21 171:10,13,16 172:18,19

affixed 128:21

affixing 128:10

afford 141:2

afternoon 3:5,7

afterthought 107:13

against 71:10,11 107:6 117:15 146:11 153:9

agencies 15:19 33:12 35:19 36:20 38:11 41:4 82:17 85:21 96:2 123:19,21 125:6 129:14 132:19 133:11,12,19 140:11 142:16 170:8,15 171:8,12 172:13

agency 13:9 28:17 29:7 34:3 40:22 41:5,6 54:9 64:17 82:15 85:19 94:8 95:1,5,16 99:16 120:9 128:12 129:7 130:6,11 133:17 136:20 138:8 142:8 162:11 170:11 171:6

agency's 86:21

agenda 17:11

ago 15:5 41:16 56:12 59:9 96:17 132:9,14 133:17 151:20

agreement 130:9,12

ahead 4:9 17:4,10 26:3 28:6 37:12 56:10 77:20 98:21 104:6 133:18 141:12 148:13 151:2 169:10

airplane 54:18,20 169:13

algorhythm 134:20

algorhythms 147:3

algorithm 28:21

algorithms 91:14

Alice 7:14 26:18 31:6 34:21 46:20 73:22 137:22 169:15

allow 125:22 126:2 132:5

allowing 35:13 65:22

allows 5:14 29:20

alluded 49:7

alone 51:18 113:19

already 19:17 26:7,21 27:12 37:20 48:18 75:21 85:1 89:12

93:19 94:12 105:19 108:12 114:5 119:20 122:14 130:14 135:3,20 158:16,21 159:17 163:1 165:3 168:8

alter 81:9

alteration 33:3

altered 23:7,9,13,15 27:9 28:20 29:2,5,17 57:8 101:8

am 11:20 20:14 174:8,11

amended 65:4

American 7:15 8:16 9:1,10 10:18 13:11 46:20 59:7

among 67:15 172:7

amongst 165:11

amount 118:16 149:14 152:8

analogies 85:10

analogous 66:21 85:5

analogy 79:17 85:5

analyze 44:11

Anderson 9:7,8 41:8 63:7 88:4,6 115:2,5,18 140:6 158:6 159:20 160:1,21 162:3

164:1,4 166:18

Andrew 11:5

Annapolis 9:9

announce 55:15

annually 147:19

answer 37:20 38:16 40:6 47:1 101:11 127:19 128:6 133:1 149:14 151:2 152:8 166:11

answered 56:12

answers 83:3

anybody 47:10 75:10 88:2 97:11 98:17 141:11

anyhow 161:3

anymore 101:22

anyone 38:21 61:10 103:4,5 116:19 120:14 124:22 139:15

anything 3:12 63:14 66:12,16 69:12 75:9 81:6 89:2,16 104:6 111:21 118:10,20 119:21 134:9 137:3 139:4 162:14 164:8 168:4 171:17

anything's 140:12

anyway 55:1 114:4 161:2,7 167:4

anywhere 21:22 32:1

apathetic

117:15,16

apologize 116:19 120:14 150:11

apologizes 3:10

apparent 115:21

appears 174:5

appendix 64:15

application 27:3 49:16 71:9

applications 105:4 107:18 145:5

applied 20:1 83:8 113:10 114:6

apply 18:10 72:19 84:3 112:15 153:4

applying 13:15

appreciate 4:5 7:3 46:10 115:17 122:10 163:11 164:20 168:16,22 172:22

approach 41:22 48:21 67:13 68:7 78:3 97:16 113:4,20 118:14 145:21 146:16 167:12 168:11

approached 12:9

approaches 75:8

appropriate 30:13

appropriately 74:4

appropriations 151:19

approved 144:12

April 174:22

apropos 30:2

arbitrarily 162:14

arbitrary 149:9 159:12 168:3,13

archival 31:2

archive 79:18

archived 69:17

archivist 66:10

Archivists 10:18

area 17:17 19:13 20:7 73:20 118:11

areas 20:12 51:10 104:1

arena 84:4 124:1 152:16

arenas 44:21

aren't 69:14 83:18 94:16 111:5 126:9 159:4

argues 67:9

argument 87:2 167:17

Arin 15:16

art 67:4

article 74:18

articles 129:15

ascertain 34:4

ASCII 104:13

aspect 32:20 35:6 61:12 62:9 152:10

aspects 5:7 61:7 126:6

assembled 18:8

assert 160:17

asserting 127:4

assessing 147:17

assigned 129:11

assimilate 169:21

assist 125:4

Assistant 8:15

Associate 8:21

associated 82:13 92:12 127:20 142:11

Association 7:16 8:16 9:1,10 46:21

assumed 78:12

assumes 128:17

assuming 76:19 93:18 94:12 108:11

assumption 32:2 33:4 82:5 93:17

assurance 13:2,5 19:8 23:5 27:6 28:19 33:20 49:6 102:5 141:19 144:4,15

assure 29:18 30:14 33:16,20 92:17

assured 28:16 144:9,10,13,14

asterisks 164:19

attach 64:15

attached 111:18 112:17

attaching 64:4

97:7

attachings 64:19

attachment 63:21

attachments 107:9,12,17

attending 7:13

attesting 127:4

attorney 174:12

attribute 61:18

audience 60:9 100:22 106:1

audit 99:10

audits 99:20

August 169:19

authentic 13:6,13 23:12 24:2 29:19 35:11 43:7,11 46:2 59:10 60:9 61:1 62:3,4 65:16 73:8 78:4,12,22 79:11 80:17 92:10 93:16 94:9 96:4 149:12

authenticatable 64:8

authenticate 7:11 14:6 35:2 61:11 85:18 147:2 149:9,18 167:10,20 172:8

authenticated 5:18,22 14:19 30:20 42:1 47:5,12 60:5 63:20 64:12 88:13,14 89:4,13 93:22 108:15

123:14 146:5
149:14 150:8
151:6 153:10
155:7 158:16
159:14,17

authenticating
9:21 62:6 63:1
167:5

authentication 1:9
2:4 4:4,17,19
5:6,12 6:3,4 7:18
9:11,15 10:20
11:3 13:20
14:3,9 17:14
18:3,7,10 19:8
20:9,16 22:18
23:10
24:1,8,17,20
25:3 28:12 31:5
32:12,22 33:2
34:14 36:4,11
39:5 41:11
42:16,19,20
43:6,16,21
44:8,19 45:17
47:3 53:15 54:3
55:20 58:18 59:3
61:8,13 62:9
63:3 65:3
66:15,17,19
72:13 75:3,14,15
76:6 84:3 85:17
94:22 95:7,14
101:6,16
104:2,16,17,18
106:11 108:11
113:15 121:14
127:20
142:13,18 146:2
147:16,22 148:1
149:6 153:18
171:4,13 173:2

authenticator
138:14

authenticity 12:11
29:14 73:17,18
92:8 127:21
142:9 143:20
145:3

authoritative
39:17

authorities 96:19

authority 36:22
41:6 94:5 128:17
129:9 130:11
131:16,22 132:4
134:7

authorized 40:11
41:2 133:12

automated 17:15
48:9 67:1 75:22
76:4,8

automatically
82:16

automotive 148:1

available 3:3 5:16
12:19 13:8 20:21
21:7 22:16 25:1
31:16 32:9 53:11
60:17 70:11
78:11 79:22
80:12 89:3,13
106:14 110:5
111:18 118:2
119:16

avoid 69:22

aware 5:15 21:11
45:20 48:7 71:21
111:21 120:21
172:17

awareness 17:22

121:5 146:21
147:13,15

away 143:1 156:16
162:14

B

background 3:22
4:16 12:6 17:14
20:16 22:5 41:15

bad 51:3 118:5
150:19
162:15,19 163:6

Baish 7:14
26:19,22 27:5
28:3 31:9
46:19,20 94:16
138:1 152:21
169:16

baked 53:9

band 40:8,12

barrier 66:12

base 117:16

based 12:22
24:17,20 31:10
36:7 47:3 48:5
49:6 50:2,7
51:1,17 52:4
53:16 90:16
91:15 102:19
135:11 137:9
147:2 148:9
154:19

basic 106:21

basically 43:16
50:6,7 66:8
108:18 123:6
139:16 165:2

basis 59:6

bat 110:1

battery's 85:14

bear 32:22 67:7
158:10

become 39:6 66:18
111:15 115:21
138:6 142:22

becomes 61:19
75:3 80:3 99:21

becoming 87:14

begin 159:5

beginning 25:16
106:8 117:18
124:8,17 131:1

behalf 7:21 14:15
132:21

behind 137:14

beings 164:13

believe 6:18 17:4
97:14

Bender 16:4

beneficial 142:2

benefit 42:10

Bennett 15:11
34:9 42:8,11
60:22 68:13

besides 121:15
122:1

best 9:14 18:22
46:15 48:12
50:16 82:2 83:5
99:9 104:22
120:18 122:20
126:5 135:14

beta 104:10
124:12

Beth 9:3 170:17
171:18

better 45:9 59:22 71:5 107:15,18 161:11 170:1

beyond 48:18,19 100:6 103:1 104:2 126:8 156:17

bid 156:3

bill 31:13 62:19 69:8 73:7 151:19

bills 16:17 22:9 47:17 62:18 101:18

binary 24:21 105:6 121:18

bind 43:4 130:11

binding 131:5 139:12

bit 10:5 12:6 18:4,12,14 22:5 29:18 33:10 42:14 44:22 45:16 48:11,19 52:22 53:6,10,17 54:10 72:7,12,22 84:2 86:13 87:4 96:16 97:13 98:16 104:4 108:6,16,20 114:5 123:1 125:20 129:2,22 130:18 131:13 139:7 143:5 147:12 152:4 156:9 159:15 160:14 161:11 163:15 166:19 168:10

bits 92:12

Blackberry 141:11

block 57:12 116:15,20

blocks 41:22

blow 97:6

blue 36:14 46:22 86:11

board 123:18 170:21

Bob 10:13 66:6 79:16 96:14 145:6

bodies 54:11

body 46:9 115:7,14

boils 100:16

book 53:2,22 80:8 94:2 139:12 140:10 143:17 167:22

books 41:17 86:20

Booth 8:7 37:8,11,14 39:15 57:17,20 70:6 84:10 116:3 120:3,17 121:7 122:2,12 126:20 128:1 138:19,21 139:22 164:22 165:18

born 12:20 13:21 60:14 99:16 172:2

borne 132:11

bound 53:2,22

box 151:2

boxes 77:13

Boy 67:7

branch 132:13 134:6

bread 6:17

break 3:1,6 71:14,17 72:7 88:7 103:7,12 148:21 167:17

breaking 76:2

bridge 38:19,22 132:3

BRIEBE 71:18,21

brief 45:19 64:1 98:1

briefly 96:14 145:22

bring 3:22 4:21 6:10 32:19 46:16 99:4 158:10 166:5

bringing 99:7,12 136:6 157:14

brings 89:10

broadly 39:8

broken 45:8 100:13 134:21

brought 33:13 67:7 73:22 104:9 146:22

budget 22:7 39:9,18 40:1 124:13,14

build 117:13 157:2

building 57:12 124:5

builds 56:21

built 94:10 107:14

bulk 73:13,14

bullet 23:5

bullet's 24:22

bunch 15:19 146:12

burgeoning 151:17 152:1

burning 77:7

business 2:21 7:9 12:3 23:19 46:11 49:16 51:19 52:12,17 53:3 93:10 96:10 97:9,16 145:11 164:13

busy 169:1

button 26:6

buying 13:3

bytes 43:20 50:10

_____
C

cache 117:5

cafeteria 3:3 103:10

canvas 148:5

capabilities 4:21 49:19 69:1 87:14 96:2

capability 51:21 126:4 152:13 165:5,6

capable 5:17 47:6 104:11

Capitol 1:13

capture 63:18

captured 35:11

48:20

card 39:11 132:12,15

cards 3:15

care 91:17 92:2 93:4 97:4,22 100:1 114:18 124:22 136:15

careful 125:9 164:19

carefully 36:10 152:7

carried 128:20

carrier 104:11,17

carry 14:9

carrying 166:3

case 2:14 8:11 38:8 63:21 64:4,11 73:22 76:14,19 77:1,2 79:7 84:7 86:12 99:6 101:3 102:4 113:10,13 117:14,16 126:5 129:12,17 154:1,8,14 155:1,16 156:20 159:8

cases 12:20 17:21 60:15 67:3 73:3,5 74:6,22 75:12 76:2 100:16 106:15 113:6 123:1 126:6 129:4 134:13

casual 36:12

catalog 137:5,6,7,9

caution 107:6

120:10 158:7

census 34:19

Center 11:15

central 15:17 131:15,22

centralized 35:16

centrally 82:15

cert 124:16

certain 49:19 69:20 71:10 96:8

certainly 36:4 38:20 47:17 83:2 104:11 114:6 134:13,15 156:11 161:13 164:3,9

certificate 39:11 40:1,2 41:1 96:19 131:6 134:7 146:7 174:1

certificates 61:5 84:12 130:21 131:10 132:16 133:16 146:12

certification 132:4

certified 38:18 134:2

certifies 132:22

certify 174:4

chain 13:22 14:1 17:21 20:1 23:12 25:14 27:10 29:3,7,20 35:12 38:1,19 39:3 41:10 42:22 43:12 46:2 47:12 52:3,8 73:18

79:13 80:15 94:7 98:4 100:12 113:14 114:8 123:1 124:8,15 125:13,18,22 126:15,21 129:19 132:18 135:7,22 136:15 138:3,7,11,17 140:13 142:10 143:2,5,9,16 144:19 172:1,3

chain-of-custody 134:13

chains 27:4 92:17 113:19

challenge 13:7 38:5 91:11 147:3,7,11 149:5

challenges 13:19 14:10 40:16 58:1 95:8 148:3 160:7

challenging 63:4 148:12

chamber 55:8

change 29:15 40:19 81:11 131:8 145:15 147:3

changed 81:9 86:5,7

changes 69:3 125:8 147:22

changing 147:15

channel 49:9 88:1 89:3 92:1 99:13

channels 86:6 99:19 102:16

chapter 168:1

chart 150:13

chatting 125:5

cheap 110:4 139:10

check 29:1 32:12 57:1,2,3 90:22 91:19 117:22 146:11 153:18

checking 91:19

checklist 3:17

checks 91:8

checksum 28:21 29:2

checksums 29:9

Chicago 11:9 58:16 77:10 92:4 142:7

Chief 4:15 14:14,15

child 109:5

children 45:12

chime 103:5

choice 84:17 91:17 149:4

choices 28:1

choose 38:4 120:1,4 122:8 132:20

chose 106:9

chunks 167:18

churn 131:7,9

circumstances 31:3

citation 35:2 62:16 165:13

cite 13:12 34:17

59:15 90:12

cited 90:5

citizen 48:9 53:12 59:7 66:22

citizens 18:22 21:18 59:13 107:1

claim 83:2

clarification 82:3

clarify 58:10

clarifying 55:10,18

class 56:15 112:3

classic 136:1

clear 25:4 43:14 100:2 102:14 117:1

clearly 40:1 89:8 126:2 152:3 161:17

clever 54:15

click 46:7 151:10

clicks 25:6

client 53:11

clocks 71:18

close 21:13 99:2

closely 15:2

closer 71:19

closet 62:13

code 20:22 63:19 65:12,13 85:22

codes 21:2

coding 52:12 111:8

coffee 168:17

Coggins 8:20

collaborate 158:2

collaborates 7:10

collections 7:12 22:14 94:19 137:8

collectively 172:12

COLUMBIA 174:20

column 51:5,13 58:8

comes 16:9 17:5 54:8 59:18 92:8 128:8 146:5 149:22 150:22

comfort 89:20

comfortable 48:14 98:8 140:20

coming 2:3 5:6,16 7:2 12:5 36:20,21 37:4 41:6,14 59:8 92:9 94:8,20 99:14 100:1,7 130:7 167:1,2 172:22

command 112:14

comment 31:17 33:8 37:15 45:1,20 46:11,19 48:3,6 55:9 66:21,22 67:8 84:1,11 97:20 98:1 115:6,16 117:12 119:11 125:20 160:22 163:12,20

commented 135:20

comments 38:18 59:1 63:9 68:4,5 96:13 117:14 137:15 153:14 162:11 165:1 166:6 168:16 169:9

commercial 32:9 35:20 36:14 153:17

Commission 174:22

Commissioners 10:19

committee 96:20 142:1

common 57:20 113:20,21 119:5 132:5

communicate 148:17

communicating 123:20

communication 40:15,19

communities 21:10,13 72:14 122:3

community 6:11 7:19 19:7 23:1 30:14 46:17 48:13 49:11 50:16 59:4 78:5 81:13 83:5 84:21 93:5 94:11 130:18 140:4

companies 46:5

companionable 34:5

comparatively 44:11

compare 55:3

compares 49:13

completely 65:21 95:9 110:15 125:18

complex 89:9 114:9,11

complexity 25:9 102:18

compliant 118:21

complicated 19:12 49:11 97:14 110:10

complications 70:1

component 10:11 153:11

components 7:19

compose 91:5

compromised 134:20

computational 57:15 91:18

computer 8:4,8,9 11:16 56:15 64:13 107:10 139:15 146:4 147:8

Computers 11:15

Computing 45:9

concept 43:18 52:18 56:2 57:5,9 70:17 81:15 83:6 87:19 89:9 96:6 102:22 105:10

109:4,11,17
123:3 125:6
130:4 149:16,17
150:3,5,14
152:22 154:11
155:15 157:8
159:16 161:14
166:1

concepts 44:21
151:16

conceptualizing
5:11

concern 36:2 93:8

concerned
20:12,13 44:3
71:3

concerns 162:10

conclusion 104:22

conclusions 113:2
114:15

conference 4:10
10:18 26:17
122:18

conferences 2:14

confidence 98:11

confidential 70:8

confidentiality
127:21

confused 87:4
111:15

confusion 23:1
42:14

congress 8:18 9:4
11:6 15:1,2
16:9,13 22:9
27:19 65:1,7
69:10 99:18
138:9

congressional 8:12
16:7,11,15,17
22:9 47:17 63:19

congruences 145:4

conjunction 74:8

connected 24:12
56:8

connections 97:9

cons 108:20 110:3
120:6 128:5
130:19

consensus 18:20

consequences 78:6

consider 106:5
113:13 155:4

considerable
67:16

consideration
64:18 155:9

considerations
118:1 134:14

considered 65:5
116:21 122:4
154:17 155:8

considering 26:1
63:10

considers 82:6

constituencies
18:16,22 46:14
67:14

constitute 65:9

consultants
170:21

consumer
36:3,7,13 98:10

consuming 168:14

contained 69:11

contains 29:19

content 5:7 7:10
10:12,16 11:2
13:15,21,22 17:2
19:9 20:3 22:4
27:14,18 29:20
30:20 33:22 38:3
56:3 60:14,17
68:14 72:20
73:3,15,16
74:9,14
75:1,2,4,12,17
76:15,16,17,22
77:2 78:12,20
79:21 83:17 90:3
99:7,8,10,12,14,
15,16
100:8,9,10,19
101:6,7 104:9
109:6,14,19
110:9,12,15,18,2
1 111:1,4,13,16
113:11 114:4
123:7,14,17
124:6,7,19 129:6
141:14
144:8,9,13
147:2,18 149:18
153:5,9,13
155:8,13 166:20
167:3,6

context 39:1 67:10
111:10 155:5,8
161:2,8 163:17
164:10

contexts 146:4,15

continue 6:5 14:17
103:2

continuously
147:16

contract 130:9

contractor 38:21

contrast 55:3

control 33:6,14
81:16

controls 90:10

conundrum 143:1

convene 71:16

convenience
159:13

conversation
103:3 143:11

conversations 6:21

converted 74:10
99:17

convey 113:19

conveyed 99:22

conveying 73:17

convoluted 25:5
140:16

COOKS 16:1

cool 158:9

coordinate 114:5

coordination
27:14 114:3

copies 35:14 42:1
88:11,13
139:10,19

copy 61:3 102:3
143:21 158:18

copyright 77:17
81:9

corner 26:5

correct 31:3 88:19
102:6

co-sponsor 42:18

cost 102:15
    135:8,9

costs 89:8 111:7

Council 7:7 11:10

counsel 174:9,12

counts 53:13

couple 2:8 9:13
    21:4 38:17 105:6
    149:8 168:19

coupled 110:7

course 27:9 57:12
    71:7 88:19 95:8
    98:3 135:8
    145:11

court 32:8 47:14
    64:3 73:10 74:5
    86:3,8 138:7,9
    153:7,15 174:1

courtroom 47:6

courts 47:21 63:12
    65:8,18 138:4

cracks 134:19

craze 45:10

create 62:18 69:8
    91:6

created 69:11 79:5
    158:21

creating 46:12
    69:12 116:5,6,10
    137:8 157:21

creation 141:8
    170:11

creators 124:7

crisis 12:10

criteria 26:12 84:5

critical 31:11

cross 10:1 38:18
    134:1

cross-certified
    134:5

crowded 103:11

CRS 15:2

crucially 31:14

crypto 156:10

cryptographic
    44:1 49:8 54:14
    56:5,16,18 57:12
    58:7 91:3,15

cryptological
    134:22

crystallized
    135:17

culinary 92:20

cumbersome
    140:16

curious 150:18
    169:16

current 19:10
    76:5,11 95:17
    113:4 131:14
    147:14 151:20

currently 131:16

curve 59:21
    133:18

custodial 77:11
    78:16
    81:14,15,19
    92:17

custody 13:22 14:1
    17:21 20:1
    23:12,13 25:14
    27:4,10
    29:3,7,20 35:12

38:2,19 39:3
41:11 42:22
43:12 46:2 47:13
80:15 94:7
113:15,19 114:9
123:1 124:8,16
125:13,18,22
126:15,22
129:19 135:7,22
136:16
138:3,7,12,17
140:13 142:10
143:3,6,9,16
144:19 172:1,3

customer 13:3
    59:5 153:3

customers 129:7

cut 103:4 159:11

cuts 149:20

cyber 31:11,13

cycle 5:13 7:17
    63:10,21 64:8
    124:9

————————
                D
D.C 1:14

D.N.A 97:6

daily 59:6

Dalecky 11:20
    68:6 72:10,17
    76:13 77:14 79:2
    89:18 99:1,4
    101:1 128:7
    143:10

Daniel 15:9,11
    34:9 42:11 53:19
    68:8

data 4:17 15:4
    19:2 22:11

24:21,22 25:8
29:5 30:15
34:14,19 35:20
36:3,8,19,20
49:3 73:11 77:3
79:11,15
80:12,16
82:5,6,14,16,18
89:21 90:1,9,22
98:10 105:5,6,11
106:22 107:16
110:20
112:13,16,17
113:17 120:21
123:12
126:1,2,16 127:1
136:5,9 137:1,8
144:15 148:5
154:9 160:4
161:15,18
163:14 167:18

data.gov 34:11
    73:14 77:3 78:14
    79:6,8,10,14
    80:13
    82:10,13,16,20
    96:3

database 47:9
    153:17

databases 47:8

date 85:17 169:17
    171:22

dated 28:1

David 154:20

Davis 7:9 12:1
    40:21 59:2 60:7
    78:2 80:10
    106:3,4 124:4
    127:18 134:4
    154:20

day 6:9,10 15:6

50:19,21 98:9 116:8 169:1,17 170:4

days 2:21 169:5

de 30:5

dead 85:14

deal 23:2 37:6 43:5 54:19 68:17 92:15 93:3 109:22 158:20

dealing 13:20 68:16 92:7

dealings 142:16

deals 155:15

Dean 8:21

decent 103:16

decentralized 67:19 95:9 146:2

decide 50:15 75:5 121:14 157:22

decided 69:7

decision 18:21 19:6 25:10 29:21 50:15 80:6 81:22 120:9 148:19

decisions 18:17 78:10 87:13 95:21,22 96:3 135:11

deemed 74:20 78:21

deep 34:2 60:8

defense 11:12 45:3 98:2 107:5

define 20:10 97:11

definitely 126:17

157:18

definition 116:14

definitions 60:8

definitive 23:2 121:18 150:7 164:11

degree 20:5

deliver 6:20

delivering 153:2

delivery 11:19 73:19

demonstrate 99:19

dense 74:14

deny 128:4

Department 8:5 11:11 37:1 40:11 45:3 94:21 107:5 133:13 137:11

depend 166:19

depending 39:13 71:8,9 127:14

depends 119:16

deployments 18:18

deposited 99:15

depositories 146:7

depository 7:7 9:16 12:19 92:9,11 94:6 142:12 143:17 144:12,14 146:3

Deputy 12:8

description 95:3

descriptive 164:11

design 167:12

designated 41:5 65:7

desired 18:13 87:18

desires 77:7

detached 108:19 110:14 112:5,8 114:10 115:8 116:14,16,21 117:7 118:15,17 119:2

detachings 64:20

detachment 115:10

detail 14:3 60:8 170:2

detect 21:21 23:14

detecting 23:8

determine 37:17 89:21 110:20

determining 39:17

develop 75:7 108:5 115:13 171:1

developed 145:13

developer 117:16

developers 112:14

developer's 117:21

developing 107:12 115:12 145:8

development 17:1 166:19

DHS 31:13

dialogue 70:16 75:20 81:21 83:1 87:7

dictate 123:17

124:1

dictionary 29:6

differ 75:5

difference 53:10,20 60:4 67:16 110:17 156:15

different 14:1 16:8 18:19 19:8,20 20:2,12 25:6 32:20 44:18,19 46:5,14 48:5,11 49:12 50:14 52:2 60:3 67:3,13,14,15 69:21 74:22 77:5 81:21 84:12,13 86:11 101:15,17 102:12 107:20 108:16,18 110:8,9,12 117:8 123:9 127:8,13 130:7 131:9 139:9 141:13 143:6 145:4 146:12

differentiating 58:13

differing 36:7

difficult 106:10 120:7 146:9

dig 120:11

digital 5:9 7:13 9:5 10:10,11,16,21 12:10,20 13:15,17,21 19:10 20:19 22:12,15 29:6,15 30:3,5,10,15,22 32:21 33:3,4

39:11 44:1 47:3
48:21 49:8
50:9,10 51:9,20
52:8,14 53:5,15
54:4,15
56:5,16,19
57:3,12 60:14
61:5,22 65:21
83:6 84:22 85:6
88:15 91:3,16
92:14 93:3 96:18
99:16 105:11
108:17 110:19
124:16 128:3,10
132:16 133:15
137:8 138:2
139:8 141:9
172:2,5

digitally 5:14 13:8
20:18 29:9 78:21
82:5,17 124:7,11

digitization 9:5
170:11 171:1,20

digitized 13:22
172:5,9

digitizing 172:12

diligence 92:16

diminishing 61:16

DIP 10:15

direct 28:14
73:6,21 104:16

direction 39:14
58:17

directly 86:21
143:18

director 7:15 8:15
9:8 12:3 16:2

directory 73:14

disadvantages

104:14,15
111:3,9 119:15

disappearing 7:20

disconnected
24:9,13

discuss 13:18 71:1

discussed 72:12
171:22

discussing 45:13
81:7

discussion 5:22
14:12 17:12
20:11 37:3
72:11,18 75:11
81:5,16 95:13
102:19 106:8
125:12 126:11
140:8 143:12
172:7

discussions 47:22
78:9 98:19
152:22 155:2

Disease 10:4

display 25:4 36:10
155:22

displays 36:14

disseminate 23:2
78:5

disseminated
22:15 75:16
80:20

disseminating
19:17 20:17
105:20 108:12

dissemination
20:4 88:1

disseminator
22:20 25:4 51:14

distinction 129:18
138:1

distribute 77:18
128:11

distributed 35:18
67:20

distributing 36:22
129:1

distribution 9:16
129:10

DISTRICT
174:20

dive 78:14

diversity 48:6

Division 8:10 11:2
16:5

document 1:9 2:3
4:4 22:20 23:6
25:5 27:7
28:13,16,19
29:14 33:1 34:4
39:19 42:2
43:7,17,22
44:1,20 45:4
51:14 52:20
53:21 56:11
57:6,7 59:10
61:15 62:3,6,7
63:11 64:5,21
95:15 97:8,11
107:21 109:7
110:16 113:22
116:17 117:19
125:14,19
126:1,18 127:9
128:13 129:9
133:2 136:22
137:1 139:17
140:14,21
144:3,19,21

145:1 149:9,12
150:2,6 151:4
155:7,9 159:9
160:18 161:7
162:20 163:13
165:7,12,15
168:8 173:1

documentation
99:20 133:3

documented 99:8

documents
5:19,21 10:21
12:2,10,22 15:14
16:18 18:8
22:19,21 29:17
34:1 35:5 36:22
37:4 38:20 39:5
41:2,14 43:11
61:20 62:4 63:5
72:14 82:12
111:1 116:6,7
117:3 128:15
129:2 130:16
139:8 163:22
167:1,2 171:3,21
172:2,5,9,11,12

DOD 118:12,22

done 45:5 47:2
62:4 74:7 96:10
100:3 148:22
149:1 157:16

door 2:10

dovetail 65:2

dovetails 37:22
163:20

download 32:6
73:13 101:20
167:21

downloaded 90:22

downloading

117:6

downstream 78:13 109:16

drafted 42:12

draw 58:19 62:8 74:13

dream 67:13

drive 75:13 128:2

drivers 130:20

driving 92:20

due 92:16

Dulabahn 9:3 170:7,13,18,20 171:19

duly 174:6

dump 90:6

duplicate 42:1

duplicates 88:9,17

during 64:9 88:7

———————
E
———————
earlier 12:7 19:1 44:3 48:7 52:22 53:19 66:22 68:8 90:17 92:20 94:1 95:20 115:6 123:11 128:9 136:13 147:1 153:14 162:8

early 5:10 59:21 60:13 72:18 134:5

ease 106:17 109:16

easier 115:18 145:19 161:12

easiest 69:9 119:2,3

easily 21:21 23:8 25:16 27:13,17 40:17 51:21 88:18

easy 21:17 36:11 42:3 53:13 54:21 56:7 91:4,7,9 108:2 111:14 124:6,22 127:19 135:8,10,11,12 149:6 163:20,21

echo 55:7 96:15

eCitizen 15:12 34:10 42:12

economically 142:12

ecosystem 30:11 49:1

editorial 140:18

eDOCS 129:13

education 40:15 123:18 125:4

educational 59:16 124:18

effect 41:11,12 106:6 116:6,10

effective 6:21 48:22

effectivity 151:17 152:1

efficiencies 57:14

efficiency 57:15

effort 59:3 83:7 102:18

efforts 9:1 15:14 34:12

e-filing 63:16 64:9

either 25:17 38:7 66:16 73:9,15 84:17 105:13 121:16 134:17 148:21 149:7 170:2

electronic 4:17 7:17 18:8 20:4 21:19 23:3 31:16,21 32:11 33:1,15,21 34:4 35:4 40:14 42:13 43:1,4 44:16,19 47:5,19 53:14 62:15 72:20 78:22 79:2 81:13 87:13 88:1 89:13 96:5 129:1 144:1,2 153:15 157:20

electronically 33:12 44:15

element 108:1 116:15

elements 127:22

elephants 156:12

eliminating 9:18

else 32:1 63:14 64:5 69:12,18 98:17 103:5 127:6,7,11 134:9 154:12

email 129:16 169:9,14

embed 116:9

embedded 35:4 104:15 109:4 111:10 126:1

emphasize 96:16

employed 174:9,12

employee 38:21 39:10 174:11

enabled 42:4

enacting 47:4

encapsulate 104:12

encapsulates 14:6

encompassed 63:9

encrypted 112:7

encryptographic 20:18 34:15 61:14

Encyclopedia 94:3

Energy 137:12

engaged 170:21

engagement 52:21

engaging 15:7

engine 59:18

Engineering 16:5

engines 156:22

ensure 60:10

ensuring 12:10

enter 39:5 81:15,16 151:4

entire 14:6 34:11 62:7 125:13 156:13 159:2 163:3

enumerate 121:3

envelope 108:19 109:3 113:5,20 114:7,12,13

enveloped 112:12

118:14 119:3

envelopes 110:2

enveloping 108:19 109:17 112:12 114:10 119:2

environment 12:16,22 13:2,20

envisioned 88:16 140:9

envisions 63:15

equation 51:4

equivalent 9:20 12:21 60:15,21 116:15

errand 149:19

errors 71:3

e-signatures 42:13

especially 114:19 130:6 146:12 148:9 172:9

essays 59:14

essentially 56:4 109:5,10 132:4 140:13 141:12

establish 84:11,13,16,22 124:8 145:19

established 24:18 84:19

establishes 144:21

establishing 96:18

etcetera 63:20 68:18

Europe 68:16

evaluate 154:12

event 7:22 8:2

events 147:2

eventually 45:8,10

everybody 2:2,5 3:14 4:9 5:6 35:16 70:11 72:6 101:7 103:16 115:3 140:19 168:16

everybody's 24:6 48:14

everyone 15:7 21:12 46:12 103:9

everyone's 6:22 87:15 125:7

everything 32:1 61:9 90:16 143:2 146:10 165:3,19 166:4

everything's 109:9 118:21

evidence 65:5,9 66:2

evidentiary 145:12

exact 51:15 58:6 83:16 154:2,6,14 156:9,22 160:8

exactly 44:9 82:22 110:18 111:13 134:12 154:7 155:17 170:5

examining 105:1

example 27:19 34:1 36:8 46:17 61:3 67:17 69:9,10 78:15 79:9 83:13 89:22 96:17 111:17 117:4,7 129:6

138:4 154:21,22 163:7 172:9

examples 112:1 147:5 150:19

except 160:3

exchanging 142:17

excited 8:1 15:5

exciting 4:20 103:18,21 152:21 153:12

excuse 65:1

executable 117:6

executables 107:9

execution 158:8

Executive 132:12

exist 62:19,20 77:16 121:1,4,5 125:16

existing 90:18 110:3

exists 64:5

expanded 13:16

expect 6:6,8 58:18 79:12 119:18

expectation 158:13

expected 48:4

expensive 19:12

experience 21:17,22 22:2

experiences 111:8

experiencing 143:4

expert 11:13

expire 45:11

expires 45:9 174:22

explain 162:17

exploratory 142:3

explore 72:21 81:21 153:20 154:18

extend 2:5 144:7

extending 144:16

extensibility 36:5

extensible 25:14,16 38:7

extent 9:22 36:6 91:13 98:9

external 62:4 134:14

externally 35:7 62:1

extra 107:16 125:7

extract 107:20

extremely 66:13 144:22

eye 150:13

eye-opener 41:17

--- F ---

faced 9:18

faceless 23:3

facet 125:3

facets 49:13 81:22

facilitate 51:6 78:4,12 81:12 91:16 96:4 109:13 123:10 124:1

facilitated 96:9

facilitates 109:11,12

facilitating 38:7 49:10 52:3

facing 13:7 14:11

fact 30:9 31:12,22 34:5 39:9 47:15 79:7 116:5 147:1

facto 30:5

factor 36:16 58:14 66:8 169:15

factors 23:21 36:1 50:14 55:2,5 125:11

fail 154:10

fair 54:1 156:16

fairly 27:17 48:22

fake 62:18,19

familiar 44:13 116:19

famous 10:6

fantastic 10:1

fast 72:2

faster 45:10

favor 117:16 118:4

FBLD 12:4

FDsys 7:12 11:19,22 22:11,13 28:5,11,14,15 32:7 39:6 58:18 60:18 78:20 85:22 94:20 95:3 99:6 124:6,12 129:6 153:5,10

feasible 157:8,9

features 21:8 51:12 109:15

federal 5:9 7:6,13 9:19 10:10 11:10 12:17,19 13:6,16 16:7 22:12 27:19 30:20 31:21 34:11 38:18,21 39:9 40:10 41:4 47:21 60:16 63:19 64:17 67:17 69:7 74:8,11,12,20 78:18,19,20 79:1,3 82:8 83:14,22 84:7,8 94:8 95:9 105:18 124:13 129:13,15 132:3,7,12,14,21 133:11,22 134:2,6 142:17 158:18 159:3 170:8,11,15 171:6,12 172:13

feedback 2:15 4:1 6:12 18:15 19:13 20:8 21:10 26:3,16 77:15 104:2 105:13,22 107:3 120:5 122:11,19 123:3 124:20 126:8 135:6 149:17 150:15 157:6,9 162:5

feel 78:2 82:19 87:19 91:22 127:17 131:13 140:19 169:14

feeling 87:7

feelings 84:4

fellow 11:14

felt 152:15

fewer 167:1,11

field 94:5 137:7 157:21

fifth 14:16

figure 122:17 140:4 159:21

figured 26:7

file 14:6 28:15,22 29:10,11 32:11 53:2 64:11 89:12 90:12 99:17 101:20 104:12,19 106:13 109:5,6,7,21 117:5,20 126:3 144:1 151:12 159:18 160:9 163:2,3 164:8,11 166:2 167:10

files 20:18 22:15 48:20 104:3,13,15 106:6,17 107:16 111:10 117:8 118:17 124:13 125:21

final 105:19 129:9

finally 64:11

financially 174:13

finding 41:16 59:11 135:2

fine 115:2 126:16 164:20

fined 136:10

finer 4:3

firm 41:15

first 2:11 12:12 17:13 19:7 22:1 27:12 39:9 42:12 50:17 51:9,10 52:19 59:17 76:3 78:8 105:9 109:20 124:12,21 125:20 129:6 140:14 150:16 156:21 157:4 168:20

fist 124:11

fit 80:22 111:22

fits 67:12 140:3

five 2:21 59:9 60:2 71:18 72:3 147:5 151:8

fix 101:22

flag 146:1,15

flexible 141:2

flip 26:9

floating 139:19

flow 7:12

fly 42:4 156:11

focus 18:7 145:20 171:19

focused 54:3

folks 2:22 3:16 15:13,21 17:8 22:11 46:13 55:7 126:12 128:5 130:1 146:13 149:1 169:22

171:10

font 150:13

fool's 149:19

Force 10:19

foregoing 174:4,5

forgive 51:15

form 15:3 19:2
30:10 34:5,14
100:9 132:15
137:18 142:18
171:10 172:5,19

formal 115:9

format 5:16
19:17,18,19 25:8
29:10 30:4,5
32:21 36:11
65:21 77:5 80:12
109:14 110:12
116:9 121:15
124:12 160:4

formation 171:7
172:16

formats 24:21
25:1,2 28:1
104:10 105:8
106:13 110:9

formatted 139:17

forming 171:4
172:17

forms 24:22 31:16
72:13

formulate 122:20
149:7

forth 172:1

fortunately 9:20
148:2

forward 2:6 13:19
14:9,12 15:7

18:2 21:3 36:15
75:6 76:12 87:9
122:21

fostered 145:2

Foundation 15:12
34:10 42:12
98:13

foundational 5:7

fourth 51:13 81:17

Fox 10:6

FR 74:7,17

fragile 30:22 31:1

fragment 61:19
165:7,10,15

fragments 165:8

frame 6:4

frames 75:19

framework 67:11
84:18,19

France 47:4,7
73:22

frankly 141:1

free 21:1 53:11
78:2 169:14

freely 25:1

frequently 147:19

Friday 1:12

friendly 47:9
74:2,13

fronts 67:6

fulfill 130:5

fulfilled 130:12

full 6:16 124:15
125:22

fullest 45:5

full-text 156:22

fun 4:20 103:19

function 23:19
66:16

functionality
107:13

functions 43:19
66:14 67:14,18

fundamental
125:17 135:13

furthering 81:4

future 4:4 6:21
18:18 43:3 69:14

fuzziness 156:10

fuzzy 154:4

——————
G
——————

gain 157:8

Gallucchio 11:11
45:2,22 107:4
111:19 112:2,5,9
118:12 119:6
167:16

gather 123:2

Gazette 47:5,8

geared 33:2

gears 122:22

Gee 8:17 64:22

general 33:22
39:18,22 156:1

generally 21:14
162:7

George 10:7

get-go 22:12

gets 42:2,18 43:20
45:8 53:2 61:10

63:4 64:10 68:13
86:13,17 87:1
103:11 128:8
148:12 153:6,14
155:22 161:15
162:12
163:11,17

getting 7:11 13:5
45:9 59:14,22
69:17 75:12
85:20 87:4 88:12
101:19 102:5
116:18 123:7
146:9,10 149:13
155:12 158:17

given 47:15 89:3
119:20 120:1
158:9 160:6
162:13

gives 29:10 44:17

giving 93:19 94:12
132:1

goal 23:9 45:5
95:16 145:16
149:13 161:14

goals 22:17 23:19
25:12 27:3 31:17
32:5

gone 21:15 27:16
80:4 133:14
160:10

Google 31:22
59:18 98:5,6,7
152:4,5,6 153:7

Googled 13:9

Google-type 47:9

gotten 21:9 29:4
34:6 59:9

govern 115:9

government 1:6 5:5 7:15 8:15 13:1 14:19 31:15 34:11 35:19 40:21 60:11 69:7 95:9 118:20 119:1 128:10 129:1 132:1,7,12,14 137:13,19 138:22 139:3

government's 131:14

GPO 2:4 3:2 4:5,15,18 5:2 7:8,21 8:19 10:10 11:1,17,21 12:2 13:8,15 15:2 16:6,12,16,20 18:8,11 19:13 20:6 21:20,21 22:7,14,20,21 23:1,7,14 25:20 27:7 28:11 29:13 30:8,18 31:20 32:7 33:9,11,14,16 34:22 35:8 36:21 37:4 38:5,10,12 41:1 44:12 46:14 47:2 51:1 54:7 55:8 58:17 59:2 60:1,17 64:5 66:4 68:6 72:10,18 73:4 74:10 76:9,19 77:3,7,11 78:3 79:12 80:10,20 81:1 82:5 83:3,8 85:16 87:6 89:18 90:21 94:20 96:7 98:10,17 100:1 101:13 105:18 106:3,4 107:1 114:4 115:7 121:13 123:12,17,20 124:4,11 125:2 127:18 128:7 130:14 133:10 134:4,18 136:4 138:2,9 139:17 140:16 142:8 143:10,13,18 144:4 145:2 149:12 150:8 153:17 154:20 161:22 162:12,15,19 165:11,20 169:1 171:7

GPOs 135:3

GPO's 14:18 16:21 30:19 76:20 77:16 81:8 134:20 159:21

grab 34:19 35:5,9

grabbing 34:18

graduate 8:3 11:16

grant 10:15

granting 159:12

granular 14:2 18:3 20:9 149:5 153:8 155:7

granularity 153:1 162:21 167:5

granules 168:12

graphic 109:1

gratified 21:15

great 3:17 17:3

26:8 32:14 45:1,19 48:4 58:3,21 66:20 67:7,21 71:12 83:1 84:1 85:7 88:15 93:11 95:18 96:11 97:20 98:19 102:13 111:19 112:20 113:2 115:16,22 117:12 119:8 121:9,11 122:6 123:5 131:19 134:9 135:4,21 137:20 138:16,20 142:4,8 151:10 153:19,21 157:12 161:17 163:10 168:9 170:2

greatest 6:16

green 16:10 26:7 32:16,19

grips 172:13

group 15:4 142:20 170:8,15 171:4,10,12,17 172:7,17,19,20

groups 62:3

growing 12:9 60:2

growth 31:22

GSA 132:21

guarantee 66:10

guarantees 43:16 156:14

guess 26:2 32:20 36:1 56:14 76:4 89:20 91:13 98:1

105:12,16 117:14 134:11,16 135:1 145:20,22 156:5,8,11,17 158:22 167:8

guidance 9:17 53:14 170:12

guide 3:22 17:12 25:10 77:7 83:4 87:10

guided 25:10

guidelines 99:9 170:13,14

guy 107:6 162:19

guys 78:1 82:12 83:17 105:12 140:20 145:20 167:17

H

hacked 86:22

hall 2:9

hammer 93:1

hand 36:12 52:14 58:8 89:7 113:9 127:5,6 140:9

handed 100:20

handheld 2:16 17:5

handle 107:19 108:3

handled 88:18

handling 52:9 130:22

handout 3:19 18:15 48:17 147:6 150:11

handouts 4:12

hands 114:1

hands-off 114:21

Hannan 2:2,4 3:14
4:14 5:2 12:14
15:20 17:3 26:20
27:4,11 28:6,9
30:7 31:6 32:14
33:7,9 34:7
36:17 37:7,10,12
38:1,15 40:4,13
42:7,9 44:9
45:15 46:8 48:2
55:11 56:1,18,21
57:4,19,21
58:10,21 63:4
66:3,20 67:21
70:5,15 71:12,20
72:1,6 75:18
77:6,19 78:3
81:1,11,18 82:22
84:1 85:7,14
87:5 88:5,21
91:10,22 92:5
93:11 94:14
95:18 97:20
98:17 99:3
100:21 101:11
102:13
103:15,22 108:7
112:20
115:4,16,20
117:10 118:9
119:4,7,19
120:16 121:6,9
122:6,15 125:1
126:19 127:16
128:2 129:21,22
131:4,19 133:5,8
134:9 135:4
136:17 137:4,20
138:15,20

139:20 140:1
142:4 146:17
152:3 153:21
154:3,11,15,19
155:14 156:7,19
157:3 158:2,4
159:6,21 160:3
161:9 162:4,16
163:1,8,10
164:2,5
165:16,22
167:15 168:6
169:18 172:21

Hannon 30:8

happen 9:20 138:8

happened 29:11
96:19

happens 56:4
128:18

happy 10:14 45:18
121:7

hard 102:17
118:5,7 135:2
143:21 148:9
150:10 152:19
154:5,22
157:14,16 164:1

harder 108:6
128:3

hardest 119:3,4

hardly 118:20

Harlan 8:3 36:18
37:7 49:7 55:12
58:5 95:20
112:10 119:10
131:22

Harlan's 37:15,22
51:17 84:11
117:13

Harold 8:7 26:5
37:14 54:2 58:4
70:5,6 84:9,10
87:11 116:2,3
119:19 121:22
126:19,20
135:22 138:18
143:12 164:21

Harold's 44:14

Harvard 10:8

hash 28:21
35:7,8,16
43:19,20 44:5
49:6 50:2,7,18
51:1 52:4 53:16
55:22 56:17
57:1,2 62:2,5
90:6,15,19,20
91:14,20 93:3

hash-based
54:5,16 57:10
68:2 71:10 87:19
88:10,18

hashed 43:22
51:17

hashes 35:15 51:9
53:7 56:9 61:22
71:4

haven't 2:5 27:16
29:3 104:6 130:1
151:20,21 160:9
169:18 170:1

having 21:5,6
23:17 35:2,4
39:21 42:1,12,14
47:22 56:7
62:2,17 70:8
77:17 88:10 89:8
116:14 119:5
125:13 126:1
139:21 140:15

161:10

HDTPS 55:20

head 41:5,6 140:2
158:11

hear 4:2 6:11
19:14 26:22 65:1
115:3

heard 106:15
165:1

hearing 96:20
138:18 168:17

help 2:19 3:22
4:14
6:1,13,14,20
17:8 18:16,21
19:1,5 30:13
33:16 46:16
48:13 61:11 66:4
67:6 75:20 77:7
81:22 83:4,5
96:4 122:20
148:8 151:1
155:21 171:1

helped 15:3
169:22

helpful 54:22 63:3
122:19 125:2
130:3 131:11
137:21 146:18
166:8 171:9

hereby 174:4

here's 165:6

hereto 174:12

herself 143:15

he's 64:10

Hey 85:19 101:20

Hi 10:9 16:22 34:9
45:2

high 17:15
23:18,19 31:1
67:1 105:3

higher 111:7

high-level 105:7
133:1

high-volume
114:21

Hill 8:13

hinder 96:8

historians 59:13

historic 166:19

historical 10:14
14:18 66:7 79:16
96:15 145:7

history 140:10

hit 103:10 140:1
151:7,8,21

hits 152:1,6
155:20,22

hold 26:6 109:7

holding 7:22

hole 97:6

holistic 126:4

home 169:12

honestly 87:10
98:22 160:6,20

hope 21:15 80:1
103:8,16 153:19

hopefully 25:6
47:22 67:5 130:3
148:15 153:9

hoping 72:8
131:12

Horton 10:13 30:1
66:6 67:9 79:16

96:14 145:6,10

hosted 82:14,15

hour 72:12

House 15:13
39:10,22 40:10

housekeeping 2:8

HR1 69:10

HSA 50:7

HSPD-12 39:11
132:11

https 35:3 90:19
156:14

hub 132:2,3,4,22

huge 93:8 119:14
139:13

human 61:21
114:21 164:13

hunch 166:21

hundred 128:12

hurdles 76:5,7

hyperlinks 107:8

—————
I

I'd 5:5 39:15 41:9
84:21 105:1
109:2 134:11
159:9 171:19

ID 61:18 132:15

idea 55:21 61:1
70:18 81:16
142:19 146:1
153:12 162:18
163:4

ideal 31:18 102:15
135:6 153:15

ideally 106:14

ideas 18:19 104:21

identical 34:5

identified 130:17

identifier
61:8,18,20
62:12,14 68:9
69:3,19 70:18

identifiers 61:14
62:17 63:2
68:19,22

identify 29:10

identity 27:7 28:12
42:21

I'll 22:8 96:17
122:12 133:8
136:18

Illinois 11:9 58:16
77:10 92:4 142:7

I'm 2:4 3:12,17,18
4:14,15 5:1,4,14
6:6 7:6,8,14,22
8:3,5,7,14,18,20
9:3,4,8
10:5,6,7,9,13,14,
17
11:1,5,9,12,14,1
7,21 12:1,2
14:14 15:5,11,16
16:1,15,19,20,22
20:15 21:11,12
28:10 30:2 36:18
47:20,21 51:3,16
55:4,21 63:13
77:15 78:8 83:10
89:15 92:22
93:19 101:12
111:6 116:18
120:11,13
121:3,7 127:4
129:5 133:2

135:2
137:1,2,6,8
139:1,22 149:15
155:19 162:16
167:8

imagine 36:7
69:11 71:9 163:5

immediate 67:2

impediment 66:18

implement 46:5

implemented
122:14

implementing
120:11

implication 66:8

importance 95:2

important 14:17
19:11,14,16
23:21 31:15
36:5,6,10,16
41:14 42:6 50:14
54:17 55:2 71:3
91:20 94:8
96:6,12 97:17
98:4 101:3
111:16 124:21
125:3,14
126:9,15,22
129:1,4,17,20
130:17
136:16,19
137:13,22
140:7,8

importing 33:22

impossible 67:12

improved 76:11

inaudible 2:22
4:21 8:6 9:2
10:12,20 15:22

16:3,6,21 18:11
23:17 29:7 35:19
40:20 44:6
45:8,11 51:7,8
53:14 54:9,11
55:19 57:14,16
58:14,22 63:1,6
65:12 66:5,11
67:4 68:3 69:9
70:20 71:5 73:1
78:15 81:20
82:1,2 83:11
85:11 98:12
101:12 104:19
108:3 110:6
112:10 113:6
126:21 131:14
134:13
147:17,22
148:1,2 170:5

incentives 95:22
96:8

incentivize
141:8,14

include 35:10
107:9

included 53:14

includes 10:12
88:16

including 15:3

increase 150:12

indefinitely
128:20

indexed 13:9

indicates 86:4

indicator 123:6

INDIF 170:10

individual 39:21
48:8 75:22 107:1

130:8 138:9
167:5

individuals 17:14

industry 6:9,10
8:1 19:2
148:4,5,17
169:17 170:4

inevitably 105:5
106:21

inexpensive
139:11

info 94:15 118:9

inform 18:16
81:22

information 4:15
8:21 9:6 14:8,20
16:2 19:18 21:2
31:16 32:2 33:11
34:12 44:12,16
47:10,11,20
48:10,19,20
51:19 56:6 59:11
60:10 62:5 70:9
74:1 75:15 76:9
78:4 80:17,21
93:7 94:20 95:10
96:9 100:5
104:18 121:11
123:13 124:7,9
131:20 141:18
150:17 161:4
165:21 166:20
167:3,12 169:2
172:15

informational
90:4

information's 30:9

informing 95:5

infrastructure 9:6

39:13 133:11

inherent 57:9 81:7

inherit 104:16

initial 75:10

initially 135:15
171:20

initiative 4:20
132:13
170:13,14
171:20

initiatives 8:19
11:3 170:10
171:2

innovate 51:7

innovation 51:8

innovative
148:6,17

input 17:6,18 18:1
19:2,21 24:15
45:18 48:4,16
55:7 58:11 83:3
84:5 85:7 87:12
89:17 99:11
105:2 112:20
119:8,11,20
142:1,4 168:18
169:21 171:13

insert 21:20

inside 109:4,6

insight 4:6

inspect 29:21

instance 114:20
142:17

instantly 139:18

instead 6:18 57:18
62:2 82:14 98:13
151:20 163:4

Institute 8:8

Instruction 5:3

insuring 95:6

integrated 140:4

integrity 4:17
10:12 43:18,21
44:7 73:17,18
75:14,15 90:22
127:21

intellectual 30:3
67:10

intended 40:3

intensive 87:21

intent 81:11

inter 143:18

interaction 161:12

interest 80:15 89:6
108:12 165:14
172:14

interested 65:20
106:22 114:19
120:15 150:2
155:18
171:11,15
172:19 174:13

interesting 30:7
46:8 50:15 55:2
59:5 61:7 70:18
81:5 102:20
103:1 112:21
124:10 127:16
130:4 131:10
148:16 159:7
163:18 166:1

interestingly 44:20

interface 74:12
91:5 118:7

intermediaries

98:9 107:2

intermediary 28:15 36:9 48:10 80:5

internal 33:10

international 20:20 21:6 24:18 46:12 54:12

Internet 23:7 24:9,13,14 54:20 56:8 163:2

Internet-oriented 23:3

interpret 87:8

interpretation 79:22

intimate 93:6

intranets 15:18

intrigues 63:8

introduce 81:19

introduced 31:13 65:17 66:1

introducing 15:9

introduction 4:8

invent 51:2

inventing 145:14

investment 139:13

involve 44:6

involved 9:4 45:21 50:18,20,22 96:1 111:14 114:11,21 147:9 152:18 156:3

IP 16:15

isn't 5:15 35:16 54:18 58:1 60:4

61:1 87:9 88:22 89:2 111:15 120:14 140:3

issue 13:14 31:11 32:22 33:22 37:6 40:11 65:3 68:14 80:15 85:2,21 114:6 132:19 133:12,15 139:5,6 141:22 147:9 153:6 154:21 158:12 159:1,2

issued 124:16

issuers 132:5 134:1

issues 7:16 9:11 15:19 43:12 86:9 102:11 120:12,20 121:1 143:6

issuing 28:17 29:7

item 113:12

items 92:11 126:8

it's 3:9 4:11,19 7:3 13:16 14:5 19:12 22:11 23:7 25:11 26:21,22 29:8 30:4,5 31:1 36:9 41:1,6 43:8 44:17 45:19 46:10 48:17 52:10 53:6,18,21 54:15 57:11 59:16,22 60:2 62:11,21 66:5,21 68:4,20 71:15,19 72:2 74:7 75:21 78:7,15,20 80:12,13,21 81:4,5,20

82:8,10 83:8,20 85:13 86:5 89:1,15 90:5,7,9,21 91:8 92:15 93:7,9 97:7 98:15 99:15,16 100:1,7 101:1 102:14 107:19 108:2,14 109:6 110:7,18 111:7 112:5,12,17 114:1,9,13 116:20 118:5,6,13 119:18 120:6 122:19 123:18,22 124:10 127:8 128:17 129:11,17 130:9,14,15 132:2,3,6,10 133:20 134:15 135:15 136:16,17,19,22 138:11,20,22 140:7 141:19 142:22 144:20 146:9 147:5 149:4,6,21 150:10,13,18 152:21 153:4,11,13,16 154:17 156:2,15,17,20,21 157:1,14 158:9,21 159:21 160:14,20 161:20 163:20,21 164:1,2,5,9,14,15 166:4,5,9,10,14,

15 168:1,2 170:16 171:6

I've 4:18 9:9 10:3 11:3 14:22 37:20 83:13 92:7 93:19 127:5,10 150:22 159:9,10

— J —

Janice 16:22

Jessica 8:14 104:5 157:17

Jim 15:20 16:4

jobs 131:8

John 2:4 4:14 5:2 6:7 11:8 12:14 28:4 30:8 33:9 46:20 58:15 75:9 77:9 78:16 81:1 87:6 92:3,5 93:14 96:16 106:12 116:1 119:16 125:1 129:21 131:3 134:4 136:13,21 142:6 143:15 151:15 154:21

John's 14:3

Jon 58:7

Jonathan 11:14 35:22 40:20 48:7 55:9,17 91:12 97:21 134:10 135:17 163:11

journey 5:12 6:5 22:2 23:16,22

judge 64:10 138:4

judges 141:5

judging 98:15

judiciary 63:15

Judy 16:1

jump 28:4 54:2 78:1 88:22 106:2 123:4

jumping 113:3

June 1:12

_____ K _____

Kate 10:9 28:10 32:18 33:9 97:15 123:11 124:5

Kathleen 16:14

Kauffman 16:19

Kevin 11:11 107:4 118:11,12 139:1 146:22

key 7:18 21:4 24:19 37:1,5,6 62:18 133:10 134:20 162:15,20 163:7 167:19

keys 131:16

kick 103:17

kicked 152:12

kicking 138:12

kidding 81:19 101:12

kinds 50:8 87:8 113:15 163:21

klutz 71:6

knew 31:19

knowledge 34:2

Kodak 170:19

KORNILOVA

174:3,18

_____ L _____

labeled 40:2

Labor 8:5 37:1 40:11 94:21

lack 18:18

laid 113:3

Lance 3:12,17

Lances 4:14

land 66:2

LaPlant 11:17

laptop 3:11

large 5:20 48:9 65:11 107:1 139:14 156:20 167:7

largely 132:8

larger 22:22 67:10 123:13

last 5:9 6:15 24:22 41:19 72:12 92:7 148:20

lastly 10:3 18:2 20:9 25:13 111:11 148:4

lately 23:11

later 2:14,20 4:12 6:6,8 25:17 39:3 45:15 54:10 84:2 113:9 131:2 150:12 169:20

law 7:16 8:17,22 9:1,9,10 10:8,20 11:5,15,16 31:21 32:7 41:9,15 46:21 47:4 61:16 64:22 65:10,12

66:2 73:7,10 74:5 86:3 88:7 96:18 115:6 151:20 158:19

laws 10:19 47:16 65:6,8

lawyers 97:6 160:20

lead 31:14 72:10 171:7

leadership 132:8

leading 79:7

learn 103:3

learning 59:21

least 20:10 21:10 48:22 50:5 63:11,15 73:3 118:16,22 134:8 135:15 144:17 146:15 147:20

leave 121:12

leaves 23:14 128:19

legal 10:21 47:19 65:5,9 90:4 93:5 144:22 145:11 161:1

legalistic 143:8

legally 83:21

legislation 42:13

legislative 15:4,14 16:8 42:17

legislators 141:5

legislatures 10:17

legitimate 154:13

lend 49:19 54:4

length 24:2

les 19:9

less 44:4,5 82:18 86:20 87:20 89:1 96:1 147:5

let's 15:9,21 31:6 39:18 40:4 48:14 49:21 55:20 78:14 98:5,11,21 103:22 105:15 108:9 112:22 114:22 125:10 146:19 150:9,18 162:11,15,18

level 23:18,19 41:5 49:6 58:18 66:11 67:17,18 83:19 86:16,17 99:21 142:13 162:21 170:2

levels 13:20 14:2 19:8 101:15 129:19 168:13

leverage 141:17

Lexis 153:8 158:19

liaison 16:12

libel 80:7

librarian 10:8 92:10 93:18

librarians 59:12

libraries 7:16 9:1,10 12:19 46:21 118:5 122:13 142:13 146:3

library 2:14 7:7,9 8:16,17,21 9:4,9 10:8 11:2,6,10 12:3,13 13:4

14:21 15:2 17:1 41:9,16 59:4 64:22 79:18 86:20 88:7 93:15,18 94:18 99:17 115:6 118:2 136:14 143:17,19

lie 93:10

Lieberman 31:12

life 7:17 30:20 41:12 63:10,20 64:8 116:4 124:9

light 89:10

lightly 125:9

Likewise 14:2

limit 114:1 155:2

limitation 153:4

limitations 136:3 153:13

limits 166:14

line 27:21 33:17 34:6 61:1 66:19 112:14 172:11

link 4:11 74:3,19 104:17 111:3,4 121:8 134:7 150:7

linked 132:22

links 133:9

LIS 8:12

Lisa 11:1,17 22:10 85:12,16 101:12,13

list 4:10 29:11

listed 169:3

listen 18:2

literally 139:19

little 10:5 12:6 18:4,12,14 22:5 25:7 26:8,11,14 27:13 29:18 33:10 42:14 44:22 45:16 48:19 52:22 53:6,10,17 54:10 72:7,12,22 84:2 86:13,17 87:4 96:22 97:13 98:16 104:4 108:16,20 110:10 123:1 125:19 126:11 128:8 129:2,22 130:18 131:13 134:11 139:7 141:2 142:3 143:5 147:12 152:4,7 156:9 160:13 161:10 163:4,15 164:19 168:10

Live 5:13

load 117:22

loaded 51:17

loan 143:19

located 108:2 161:8

locating 149:11

location 68:22 165:13

locations 31:2

lock 141:15

locked 141:4

locks 88:8

logic 154:4

logical 155:11

long 4:16 10:16 29:10 35:12 41:13 45:4 62:21 66:8,12,16,18 68:12 70:1 112:16 119:17 131:4 162:20 164:10

longer 72:7 167:14

longest 41:13

longstanding 130:16

loops 95:19

lot 5:19,22 11:6 15:19 17:16,18 18:19 20:1 22:3,10 25:8 38:3 42:17 45:17 46:13 48:5,15 49:12,16 52:12 56:6 58:1 60:13 71:4 72:18 83:3 84:8 86:9 87:9 104:20,21 105:10 107:7 108:4 111:8 114:3 123:8 124:2 125:6,7 131:5 133:2,3,9 145:14 146:10,13 152:10,11 156:2,6 158:8 164:10 167:1,10,11

lots 37:17,18,19,21 38:8,9 44:17 54:10 55:5 64:19

120:1

loud 20:14,15 136:18

lower 87:20

lucky 134:22 135:1

lunch 3:1,2,4 17:20 103:7,17,20

lunchtime 98:22

Lyle 16:10 32:16,17,19 33:13

———————
M
———————

machine 69:17

main 172:6

maintain 117:8 120:8

maintained 90:10 100:12 144:4,6

maintaining 147:14

maintenance 144:14

majority 93:9

MALE 3:13

malicious 71:6,7

maliciously 29:2

manage 6:20 15:17 80:1 117:8 120:8

managed 131:17

management 5:8 7:17 11:2,18,21 17:2 37:2 59:6 68:14 99:8

124:14
157:20,21

manager 11:22
16:21

manages 12:3

Managing 16:2

manipulate 118:6

manner 85:4

map 155:6

marginal 102:18

mark 16:19
137:6,7

marks 93:3

Mary 7:14 26:18
31:6 34:20 46:20
73:22 137:22
169:15

Maryland
9:8,12,19 41:9
88:7 115:6

mash 34:20 110:22

mashed 35:1 73:15
80:13

mashup 79:22
80:18 98:10,12

mashups 77:2
102:22

master 131:15

match 154:2,7,14
156:9

matches 33:1,5
157:1

material 30:3 44:6
54:4 77:17 79:19
89:5 94:7 98:7
103:8 123:8

151:6

materials 96:5
117:11

mathematical
125:17

mathematics
147:9

matter 11:13
77:13 90:14
119:12

matters 112:11

maximize 24:2

may 29:17 37:16
38:7 40:7 49:2,7
51:16 56:14
57:17 60:22
66:14,15,17
70:10 79:14
83:16 84:11
86:22 95:19
105:14 106:22
111:21 125:5
135:10 147:1
148:7 150:19
151:6 164:9

maybe 20:12
39:21 40:6 45:12
54:17,18,20 63:9
67:10,13 71:5
79:17 85:1,14
89:16 96:16
97:3,12,13,17
102:11 104:10
109:2 112:18
114:5,12 116:4
118:22 125:12
126:9 130:2
131:10 140:3
145:12,17
149:12 152:18
160:9 161:18,20

166:15

Mayer 11:14
35:22
55:10,13,17
56:14,20,22
70:21 91:12
97:21 117:13
134:11 145:22
156:5,8 162:8,18
163:3,9

McGilvray 8:14
157:18 158:3

mean 31:10 33:7
34:18 41:21 53:2
57:6 58:5 62:9
66:10 67:16
69:22 77:11,21
79:20,21 81:15
82:9,12
83:12,13,15 84:6
88:2,11 89:6
90:15 94:22
97:15 112:12
117:2 127:2
129:5 134:13
137:5 141:10
152:3 153:11
158:8,9,11,22
160:9,15,21,22
167:9,18 172:8

meaning 61:2 82:4
84:14 147:10

meaningful
155:22

means 14:1 19:10
23:8 30:10 34:15
44:4 52:19 53:7
61:14 73:12 82:4
84:9,17,22 89:2
98:14 110:11

measure 42:4

98:11

meat 29:19

mechanism 36:11

mechanisms 90:18

media 30:22 141:9

meet 6:22 99:9
132:5

meeting
174:4,6,8,10

member 11:9
31:19

memo 63:22

men's 2:11

mention 84:21

mentioned 12:7
17:4 27:1 53:19
54:5 60:13
106:12 123:11
124:5,15
133:21,22 134:5
138:21 148:5
163:18

mentioning 55:19

met 2:5

meta 113:16
123:12
126:1,2,16
127:1,8 136:5,8
137:1,8

metadata 28:13,18
69:5 97:15

method 20:20
23:11 24:19 46:2
51:13 53:13
61:21 68:3 87:20
88:10,18
89:10,22 91:15
113:8 115:15

methodology 112:6

methods 17:16,17 18:19 21:6,7 50:7,18 51:18 52:1,4 53:16 54:17 89:8,19 90:16 114:10 125:22

mic 2:17 26:5,6,8 32:17

Michael 10:6

microphone 88:4 93:12 126:13

mics 2:16 17:5

middle 154:9 172:4

migrating 29:16

migration 15:4

mike 5:4 12:7 19:1 21:12,14 22:1 33:7 77:19 78:18 83:13 107:3 115:1 152:22 170:2,7

million 60:1 152:5

millions 139:19

MIME 107:17 121:16

mind 26:13 37:13 70:13 71:1 97:3 118:1,6 146:5 149:3

minds 95:21 165:17

minimum 80:11,14

Minnesota 10:14

66:6 79:16 96:15,17 145:7

minus 118:19

minute 71:17

minutes 71:18,22

mis 56:15

miss 3:12

missed 104:6

mission 14:19 95:1

misused 164:17

mixing 90:2

mobile 112:13

model 71:2 81:2 134:12,16 141:13 144:16

modeled 143:22

models 76:6 140:22

modified 82:11

money 38:17 139:14

monitor 59:5

months 56:12

morning 3:6 12:6 14:13 17:17 117:14 124:5,15

mostly 3:21 21:9 24:6 132:11

mouse 25:6

move 6:5 26:14 43:1 48:3,15 71:5 77:8 122:22 138:17 142:20 143:1 172:5

movement 96:4

moves 95:15

moving 40:14 119:9 122:20 146:19

multifaceted 142:22

multiple 50:20 59:1 61:15 68:5 89:8 102:16 109:8 113:7,11,13 139:9 143:5

multiplicities 145:3

muttered 96:21

myriads 139:9

myself 85:9 147:17

—————— N ——————

N/A 58:9

nail 39:4 93:1

name's 8:7 16:19

NARA 74:21 157:21

nasty 107:7

NATALIA 174:3,18

nation 95:5

national 8:8 10:18 54:12

native 106:6,13,16 108:10 121:15,16,21 122:10

naturally 49:15

nature 64:1 68:11 120:22 147:15

N-DIP 9:7

necessarily 25:15 59:19 63:13 116:16 117:2 121:1 141:15

necessity 70:8

nefarious 30:10

negative 78:6

neither 174:9

nested 142:9

net 106:6

network 56:8 146:13

neutral 44:17 70:3

newer 45:10

nice 5:21 31:19 32:10 41:18

niche 122:3

night 147:8

nine 36:1

NIST 132:7

nobody 47:20 132:1

non 127:21

non-overlapping 145:5

non-repeat 127:5

non-repudiation 128:22 129:17

nontechnical 12:12

nor 174:9,13

North 1:13 7:6 93:14 126:15 136:12

NOTARY/
 COURT 174:19

note 10:3 14:22
 65:1 123:16
 135:16 154:21

notes 101:21

nothing 120:3
 150:14

notices 129:14

notoriously 118:7

nuance 76:14

nuanced 130:1

nuances 172:11

numerous 120:12

NW 1:13

—————————
O
—————————

O.J 97:5

object 30:15 52:8
 62:13

objects 121:19

observation 49:4

observations
 104:5,7 111:11

observer 10:17

obviate 161:19

obviously 7:16
 17:12 19:12
 23:15 24:10,19
 33:14 38:5,9
 47:19 51:8 52:7
 83:7 84:8 90:16
 95:16 102:15
 122:16 126:3
 149:6 159:1

occasion 9:13

occur 147:2

occurred 162:8

o'clock 3:5
 103:7,12

offer 98:1 121:14

offering 49:10

office 1:6 5:5 8:15
 11:18,21
 16:11,12 40:22
 60:12,15 74:8
 98:7 124:13
 129:12
 137:13,19
 138:22 139:3

officer 4:15 14:15
 129:11 174:3

official 7:18,20
 13:5,12 31:20
 32:3 47:5,7,8
 53:21 59:15
 60:5,12,18 61:2
 64:2 65:8,15,16
 73:8 74:4,20
 78:22 79:3
 82:7,8,20 83:21
 84:15 85:20
 86:2,6,8,16,20
 88:10,17 90:13
 92:9,13 94:13
 102:10 136:20
 137:11,12,17
 138:6,10 141:6
 161:6,16

offline 40:7 54:13
 55:13,18,21 56:3
 63:8 64:9,17
 109:11 133:9
 146:14

OFR 27:8 129:16

oftentimes 131:7

oh 3:14 37:14 99:3
 118:11 131:3
 135:20 138:18
 151:9 158:4
 160:17

old 41:17 92:22

older 69:16 86:18

olds 59:14

on/off 26:9

ones 118:2 119:22

one's 54:15 106:4

ongoing 59:16
 77:11

online 60:17
 64:9,16

onset 10:4

on-the 136:1

open 20:20 21:6
 24:17,21 25:1
 26:3 46:12 51:5
 55:4 106:1
 109:21 114:16
 125:15 126:10

open-source 117:4

Operations 16:5

opinion 9:17 32:8
 108:6 138:7
 153:7,16

opportunities 2:15

opportunity 6:19
 123:2

opposed 24:19
 39:20 66:15
 76:15 90:11
 131:2 155:11

option 104:22
 154:17

options 44:18
 105:1,7

oracle 168:4

order 28:11 47:14
 70:12 86:1

organization 2:19
 7:22 28:9 49:18
 70:1 130:11
 131:9 171:5,6

organizations
 35:20 67:15
 139:14

orient 110:8 152:6

orientation 114:22
 132:18 136:5

oriented 53:17
 84:6 105:17
 121:17

orienting 152:4

original 80:16
 88:9,13,14 155:7
 159:5 161:7

originally 99:15
 101:5 140:8
 165:14

originate 85:20

originates 77:12

originating 76:21
 85:18

originator 123:7
 144:5

originators 7:10
 20:3 27:14 38:3
 114:4 123:18
 124:6,19

ort 39:22

orthodox 143:8

OTA 136:21,22

other-hand 136:2

others 19:10 20:13
  26:1,4,13 45:21
  91:22 108:7
  118:10 119:8
  121:20 122:5
  135:19 138:17
  145:19 154:18
  170:19

other-use 126:6

otherwise 30:6
  33:12 174:13

ought 19:19,22
  26:12 119:21

ours 24:6

ourselves 15:9
  133:18

outcome 18:13
  174:13

outcomes 87:18

outside 170:16,20

outsider 84:20

overall 4:20 83:5
  104:19

overarching 25:21
  110:1

overcome 131:6

overkill 99:5 129:3

_____
          P
_____

p.m 173:1

PACER 63:13

package 166:21

packages 107:20
  167:6

packet 104:4

page 27:1,5,6 36:1
  109:3 149:10
  154:22 155:3,10
  167:2

paper 31:2 33:21
  59:20 61:3,11
  63:5 92:14
  130:8,9

papers 120:19

paragraph
  155:3,18
  159:10,11
  166:15

paragraph-by-
  paragraph
  167:4

paranoid 107:6
  139:1

parent 109:18

Parkinson's 10:4

participant 38:22

participation
  168:21 171:8

particles 68:21

particular 34:3
  39:16,19 50:9
  53:16 54:6 63:11
  64:20 66:1 75:17
  143:20 144:15
  145:1 165:8,15

particularly 7:19
  30:18 59:4 60:20
  71:2 118:5

parties 19:3,9
  20:21 21:7 48:22
  50:19,21 51:7
  64:2 76:10 87:22
  96:10 111:14

124:2 174:10,12

partners 123:21

partnerships
  97:10

party 32:9
  50:17,22
  52:19,20 80:14
  127:11 138:13
  153:18

pass 2:16,17 32:17
  102:9

passage 162:22

passed 96:18

passes 101:9

passing 17:8

past 9:13 73:18
  141:7

paste 159:11

Pat 8:11 158:6
  166:9

Patent 98:7

Patents 98:6

path 75:6 108:1,2

patron 144:2

payoff 131:2

PC 140:15

PDF 20:17,22
  22:2,15 27:14,21
  48:20 50:12
  72:13 74:15,19
  76:6 83:17
  100:10
  104:10,17
  106:13,18
  107:12 108:3,5
  109:10 111:10
  125:21 160:5,8

PDFs 5:14
  27:11,20 107:7
  118:6

pencils 160:13

people 4:19 5:17
  6:16 20:15 21:1
  28:2 32:1 34:18
  35:3,5,9,13,17
  37:13 40:20
  42:18 47:1 50:1
  59:13 61:22
  79:18 86:14 87:3
  90:2 91:7 92:15
  93:6 94:16,19
  97:3,4 104:21
  112:13 119:17
  120:20 125:5,8
  127:17 136:5
  141:14 147:8
  148:22 152:16
  155:2 165:4,11

people's 43:2

per 116:17

percent 12:17
  92:14 97:3 99:22
  100:2 101:4
  136:13

perfect 53:6 98:15

perhaps 32:2 43:3
  162:1 165:2

period 148:11

Periodically
  147:17

permanent 7:17
  95:6

permission 85:22

perpetuity 130:6

persist 100:9
  101:5

persisting 100:19

person 12:12 14:16 39:17,20 40:9 49:17 73:6 100:20 101:10 127:3,10 128:16,18 129:8 137:2 149:22 163:16

personal 10:3 14:22 77:21 131:5

personalize 138:16

person's 128:13 130:5,15

perspective 6:1 21:5 41:1 47:17 68:12 80:11 117:21 123:16 146:1 149:11

perspectives 83:4

PGI 142:10

ph 9:7 10:15 12:4 16:1,15 28:21 40:8 50:8 55:20 74:10 170:10

philosophically 88:12

photons 68:20

phrase 83:11 92:22

physical 43:2 62:13

pick 10:2 15:9,10 24:4 38:20 87:19

picked 13:9

pictures 109:1

piece 44:16 89:4

110:19 124:19 153:9 156:10 159:18 165:15 166:20

pieces 35:5 91:6 92:12 167:11

piggyback 90:17 143:11

pile 43:20

pink 86:12

PIV 132:11

PKCS7 105:10 121:17

PKCS7s 121:2

PKI 5:2 12:11,13 20:19 38:18 132:20,21 134:2

placeholder 109:7

plan 2:22 9:21 16:5 147:21 148:4,15

planet 21:22 46:13

planning 17:1 147:14

play 40:3 127:14 128:8 152:11

pleading 64:1

please 2:17 17:6 50:4 54:1 55:16 88:4 99:3 123:5 169:10,14

plenty 24:11 26:16

plow 148:21,22

plowing 103:8

plug 3:10

plug-ins 106:10

plus 5:19 67:9 118:18

point 9:17 25:21 26:2 31:1 34:7 38:19 39:16 40:22 44:10 46:20,22 49:4 51:17 56:2 66:3 68:4 69:15,16 71:13,14 72:9 90:12 93:14 97:22 102:13 103:18 106:2 107:3,12 108:8 111:7 113:2,3 114:15 118:10 119:9 121:21 127:16 129:7 130:1 136:2 138:11 140:19,21 141:19 143:8 148:19,20 150:4 151:17 154:20 155:15,16 157:12 161:10 163:10 164:6,14 165:18 166:1 167:15 168:10,18

pointed 136:1 166:4,10

pointing 35:12

points 4:3 21:4 62:10 144:2 149:8 168:15

policy 12:12 39:13 41:3 80:11 84:6 123:16 127:19 132:5 134:15 142:22

Political 94:3

politically 142:12

pollination 10:1

portable 95:14 156:15

portion 11:19 15:17 34:19,21 61:17,18 149:9

portions 35:9 62:6 90:3

posing 77:15

position 6:18 133:17

positioned 5:10

positive 21:9

possibilities 9:22 46:16

possibility 64:18

possible 6:21 25:11 41:20 54:13,14,16 55:22 91:8 133:3 157:4

possibly 66:11 91:4

post 2:20,22 109:2 150:12 169:2

posted 4:12 34:2

posterity 141:5

potential 42:14 132:17

potentially 27:18 38:3 58:17 78:9 82:18 105:6 110:10 132:18 147:5 151:11 152:2 161:20

pour 42:4

power 26:9,10 74:11

practical 48:12 81:4 87:14 111:20 113:5 160:6 168:3

practicalities 157:7

practicality 109:16

practice 36:4 99:9

practices 9:14 120:18

pre 56:3 149:17

pre-authenticating 149:21

precise 117:11 155:12

preclude 115:7

predicated 166:9,10

premise 29:5,6 30:3,4

prepare 6:14

present 76:6 94:9 100:4,18 125:19

presented 74:18

presenting 77:4

preservation 7:18 9:6 10:11,15,16,20 29:15 66:9,13,18 67:2 95:7 130:7 171:2

preserve 29:17

preserved 125:19

President 42:18

President's 22:6

pre-signing 168:12

press 26:6 139:4,12

presupposes 158:15

pretend 10:5

pretty 4:16,20 21:15,17 27:21 30:22 44:13 50:3 51:11 53:13 74:14 75:19 98:8 102:14 114:16 118:11 146:9 156:3 158:9 164:11

prevent 76:6

preview 160:11

previous 152:22

Priebe 7:8

primarily 8:18 11:18 12:21 16:6,16 59:3 172:2

Princeton 8:4 36:18

principles 25:21 41:11 154:4

print 9:18 12:21 47:13 60:14,20 61:4 65:15 74:11 94:18 95:5 139:4 141:9 144:17 164:20 172:3,4

printed 33:1,5,14

61:9,10 65:11 74:14,16 85:4 137:18,19 138:22 139:2 140:15 143:13,17

Printer 12:8 14:16

printing 1:6 5:5 40:21 60:12 129:11 137:13,19 138:22 139:3,4,12

printout 47:14

priorities 47:19

prioritizing 145:18

private 37:5 41:15 47:16

probably 3:1 6:7 17:9 20:17 22:7 31:13 43:10 47:2 51:2,4 54:21 56:9 64:13 71:14 76:3 81:3 88:19 97:5 98:21 103:1 104:22 121:10,16 126:20 130:1 131:11,21 140:16 141:1 145:19 150:10 154:5,6 155:21 159:19 160:5,7 161:12 169:19 170:5 171:14

probing 97:12 134:12

problem 37:2 39:2 70:14 93:1 143:3

148:3,9 149:4 157:14,16

problematic 66:13 70:10

problems 6:13 53:7 76:7 95:12 146:10

problem's 93:1

procedural 132:6

process 21:2 26:4 33:6,20 34:3 38:22 40:9,12,19 45:16 52:12 53:4 59:16 62:22 64:9 70:12 85:5 99:11 106:6,9 111:4,14 114:7 115:10 123:19 124:17,18 125:4,8 128:4 140:17 141:16 144:17 161:21 170:3 171:3

processes 30:12 33:11 68:1 76:5 106:11 133:14 140:18

processing 49:17 51:19 76:1,9 87:20 105:4 110:15 114:20

processors 48:10 107:2

produce 77:18 120:19 141:14,17

produces 66:12

producing 33:15 68:14

product 13:4
33:5,21

production 16:5
33:19 34:3

productive 15:6

products 18:11
81:8

program 9:6,16
11:18,21,22
14:21

programmatically
118:7

programs 9:5
23:10 132:12

progress 14:17
47:3,16 160:15

project 16:21 74:7

projects 16:16

properly 6:4

proposal 156:6

propose 46:3

proposition 6:19

propositions 6:2

proprietary 21:5
24:19,22 25:2
51:7 70:9

pros 108:20 110:3
120:6 128:5
130:19

protect 71:10,11

protecting
144:19,20

protocols 111:6
114:11

prove 100:11

proven 30:6 146:9

provenance 123:8

proves 136:9

providable 27:13

provide 3:21 4:10
6:22 14:19 17:6
18:21 19:4
22:18,22 23:11
27:6,17 28:18,20
29:6 38:10 46:1
50:9 51:20 78:5
83:9 89:1 132:15
135:15 141:18
142:13 146:21
151:1,7,11
165:5,20 171:13

provided 21:16
23:13 27:12
28:17 164:16

provider 132:21
161:4

providers 27:19

provides 25:3
30:10 51:22
83:19 126:4
148:3 165:4

providing 23:5
27:15 28:12,19
30:19 38:6 46:4
52:15 61:13 88:1
99:18

provisions 65:4

public 12:8 13:11
14:15 31:19 32:6
47:16 95:6
128:14,21
129:14 133:10
142:1

publically 28:22
70:11

publication 13:6,8
14:7,8 16:2,17
28:20 53:17
54:1,3,6 60:18
64:16 74:15,16
128:11,21
136:20
137:11,12,17
143:21 150:8

publications
9:15,16 12:18
13:1 16:6
65:7,14 66:1
92:13

publish 90:19
139:16 141:12

published 24:18
34:22 82:11
96:17 140:15
162:12 163:2,13

publisher 28:12
32:9 51:14,15
94:5 138:10

publishing 16:11
19:17 20:17
35:19 138:8
139:8

pulled 90:8

pulling 77:2
172:15

pulse 59:7

punt 141:22

purchase 94:2

purchased 94:2

purchasing 94:1

pure 135:1

purely 71:7

purported 21:21

purpose 39:22
42:19,21 55:6
56:10 58:11
70:16 75:2 81:21
83:1,9 87:6
156:1

purposes 20:11
42:21 57:14 62:7
67:22 75:13
84:13 90:4,5
102:7 122:17

puts 77:3

putting 35:20
63:22 82:9,19
86:4 87:3 99:13
127:8 139:1
155:17

—————
Q
—————

quality 31:2 33:20

question 24:20
26:19 27:1
30:1,8 31:10
32:16,21
34:8,13,22
37:21,22 39:15
44:14 49:5,12
50:2 55:10,18
56:13 58:6,9,21
68:2,7,10 69:13
70:22 75:3
76:4,18 78:16
79:6 80:19 82:13
83:11 87:11,17
88:22 89:7,14,15
92:19,20,21,22
93:10 94:11
99:21 100:21
101:12 105:14
111:19 126:3
131:19 133:1
134:9 135:4

157:5 158:22 159:7

questions 4:1 17:19,20 36:17 59:8,9,14 68:4 70:5 77:14 83:2 87:9 88:8 97:12 101:19 104:1

queue 150:1

quick 4:8 26:19 27:1 28:5 42:3 43:14 48:3 49:22 119:10 121:12 146:20 147:10 150:9

quickly 22:8 23:8 46:19 52:16 160:21

quite 21:13 27:16 40:17 48:10 87:10 111:13 114:5 118:7 141:1 150:19

quotation 161:2

quote 62:3

quote/unquote 92:13

_____
R
radical 118:14

raise 121:4 164:5

ramp 118:15,22 119:2

range 87:12

rare 86:19

rather 19:18 21:6 24:21 92:8 116:4 145:4 167:6

169:20

rationale 66:17

raw 110:12

re 45:16 147:1,21

reach 171:14

reaction 156:5,17

readable 61:21

readers 22:19

readily 109:12 110:4

reading 23:6

ready 3:9 31:7 46:15 119:9

ready-made 51:22 52:15 53:6,9

real 6:2 37:20 49:22 62:18 67:22 85:1,3 118:1 121:12 150:9 158:20

realistically 141:3

reality 135:9

realize 45:7 59:16 114:16 118:10 123:22 169:11

realized 5:11

realizing 105:13

really 2:6 4:5,19 5:15 6:1,14,20 7:3 14:1,19 17:22 18:6,7,13,19 19:7,11 20:3,21 21:15,18 22:8 24:10 25:1,8 27:16 31:11 32:22 38:2 40:8

43:14 44:14 46:9,10,11 48:16 52:5,6,7,11 53:1,17 54:5,16 55:6 57:5,9,15 58:1,13 62:11 68:1,18 70:2 78:7 81:3 84:9 85:10 87:10 88:2,22 89:6,11 91:17 93:4 94:7,14 96:12 97:4,11 98:18 100:16 103:11 105:22 107:10,13 109:18 111:5,15,20 112:11 113:12 114:19 118:5 119:8 120:8 121:20 123:18 125:3 128:6,17,22 130:2 131:18 134:22 135:16 136:3,9,19 137:15 138:16 140:7 143:15 146:18,21 149:22 150:4,6,18 152:19 153:11 155:15 157:5,8 160:9,11,16 162:1,4,9 163:11,19 164:6,16,18 166:10,13 167:12 168:6,12,15,22 170:1 171:9 172:21

realm 85:6

real-time 151:11

reason 28:4 31:3 52:6 127:1

reasonable 13:2,4 80:2 88:11 114:1 149:14 152:7,8 166:11 167:18

reasons 23:16 106:8 133:16

reattachment 115:10

re-authenticate 148:11

re-authenticating 147:18

re-authentication 17:21 39:2 146:20

recalling 56:14,15

receipt 129:6

receive 124:20

received 29:12

receiving 13:4 28:14 33:11 143:17

receptive 125:6

recipient 10:14 13:3

recipients 22:18

recognition 145:15

recognize 69:2

recognized 120:18

recognizing 60:16

re-complicate 116:4

reconvene 3:4

record 16:7 63:19 72:5 103:14 137:5,7 157:20 174:8

records 137:9

recourse 90:14

redact 172:10

redefine 95:10

redirects 69:16

redo 24:5

reduced 174:7

reducing 23:1

redundancy 42:4

refer 143:14

reference 35:10 172:3

referenced 35:14 79:5,8 121:2 154:22

references 68:22 69:5 79:9

regard 19:5 20:3 26:2 45:21 48:13 49:1 50:16 77:7 87:10 136:8 148:8 161:13 166:6

regarding 28:1 39:16

regimented 141:16

register 9:19 16:8 27:20 31:21 40:10 60:16 63:19 74:8,11,12,20 78:18,19,20

79:1,3 82:8 83:15,22 84:8 105:18 129:13,15 133:22 142:17 158:18 159:3

regulation 47:14

regulations 40:11

rehab 148:1

reinforce 125:5

reinvent 145:16

reiterate 41:9

related 10:21 37:6 101:14 104:2 172:12 174:9

relates 65:5,10 72:13 150:6

relating 149:12

Relations 7:15 8:16

relationship 59:6 81:8 142:15 144:21,22

relationships 97:10 145:2

relative 110:3 139:11 174:11

relatively 139:10

release 36:9

relevant 64:4

reliability 32:21 83:20

reliable 21:18 29:4 30:6 65:21 83:9 93:20 94:4 144:6

reliably 23:8,13,14

relies 31:15

religious 10:21

rely 32:3 56:17 73:9 89:12

remarks 60:13 77:10

reminded 92:22

reminder 170:9

reminds 157:19

repealed 151:19

replica 83:17

replicated 140:12

report 16:18 64:16 169:6,15

reporter 138:5 174:1,19

repositories 63:1,2

repository 11:10 14:20 28:16 90:10 144:3,12 148:10 167:19,21

representation 79:11 105:11

representations 43:3

representative 83:21 96:20

representing 7:6 47:21

Republic 30:21 41:12

repudiation 127:22

repurposed 73:12 154:8

repurposing 77:4

request 59:4

require 19:7 24:12 25:8 106:9 130:21

requirement 25:6 147:22

requirements 6:3 132:6 133:20 147:15,18

requires 113:20 114:3 123:17 146:13

requiring 19:10

research 8:12 10:8 59:20 73:10 74:5 80:8

researcher 13:11

researchers 59:12

resides 32:11

resign 45:7,12

resolved 143:7

resources 96:3 121:8 158:10 162:1

respect 105:18 120:4 130:6

respects 105:17 138:16

respond 97:22

response 165:6

responsibilities 67:20

responsibility 76:20 77:12 78:17 79:10,15,19

80:3,9 92:18

responsible 10:11 30:19 39:20 79:13

rest 38:11

restate 42:10

restricted 95:17

restrooms 2:9

result 59:17 160:1

results 74:17

retrieved 144:3

retrospective 171:3

returns 61:16

re-use 79:22

reusing 90:2

revision 34:6

Reynold 14:14 30:17 33:8,18 41:10 124:14 151:15

RFC 121:2

ribbon 36:15 46:22 61:6

Ric 106:2,3,4 123:3 124:4 127:18 133:21 134:4 154:20 155:15 170:3

Richmond 8:22

Rick 7:9 12:1 21:11,13 22:21 40:21 59:2 77:22 80:10 163:18

Rick's 22:10

Ric's 142:21

rightly 135:22

risk 141:1

road 25:18 95:7 131:2 136:7 161:3

Robert 8:17 64:22

robust 19:10 39:12 44:4,5 89:1

robustly 89:4,13

role 38:10 40:2 95:10 98:4 128:14 130:5,10,15 132:8 138:2,12 171:16 172:18

role-based 130:21

room 2:11,16 3:9 4:8 6:15 31:8 86:20 91:22 141:2 142:3 143:5

root 135:13

rosier 98:16

routine 145:8,10,14,16

routines 145:18

row 50:13 54:14

rule 27:9 49:17 97:16 130:17

rules 51:19 52:13,18,21 53:3 97:9

run 3:11 79:17 107:8 156:13

running 171:17

Russell 11:1 85:12,15,16

101:13

Ruth 22:10

——————
S
——————

Sabol 16:22

sales 6:16 13:3

save 102:3

saving 140:14

scalability 158:7,12 159:1

scalable 159:19

scenario 115:11 154:16

scenarios 32:11 54:22

schema 29:6

schemes 49:6 51:1

Scholar 153:7

School 8:22 10:8

Schweickhardt 151:15,16

Schweickhart 14:13,14 30:17 33:18,19 38:14,16 40:5

science 8:4 11:16 94:3

scientist 8:8

scope 18:4,5 20:10 37:3 38:12 103:1

scraping 73:13

screen 151:2

se 116:17

sealed 13:1

search 11:19 59:18

74:12 151:6,18 152:4,5,6,7 154:9 156:4,6,18,20,22 157:1,21 159:19 165:5

searchable 74:2

Sears 7:5 93:13 126:14 136:11,18 137:5

second 23:5 40:20 49:5,22 52:20 54:14 68:2 76:14 92:1 105:9 110:19 119:3 150:4,21 155:16 158:15 161:3

secondary 70:22 81:17

secondly 124:22

section 74:18

sections 61:15

sector 12:17

secure 47:6 90:19 99:8,10

secured 99:13,18

securely 90:9

security 4:15 8:9 31:11,13 56:15 89:20 90:10,18 100:17 120:20 135:1 146:4 147:8 156:14 162:10 172:10

seeing 60:19 65:20 123:19 132:2

seem 23:21 50:14 52:14 115:7 118:3 125:15

158:17

seemed 25:20
26:12 51:10
52:1,4 53:5
83:15 122:10

seems 36:2,15
37:19 49:2 51:2
53:12 58:7
88:10,17
105:5,15,21
113:5 114:9
121:13,19
125:14 126:4
149:19

sees 95:1

segment 106:22
155:12 156:21
166:15

Selene 11:20 68:6
72:10,15,17
75:18 77:22
81:18 89:18
100:22 103:5
128:6,7 133:21
143:10 147:17
153:1

Selene's 79:6

semantic 82:4
84:14

senate 15:17 94:21
138:8

Senate.gov 15:18

Senator 31:12

send 26:16 133:6
139:18 169:11

sending 129:14

sense 25:22 43:5
52:16 85:8
105:16 108:13

131:13 134:22
136:4 151:7
152:17 162:2
167:22

sent 13:1 149:10

sentence 155:4
158:13 166:14

**sentence-by-
sentence** 167:3

separate 42:20
47:8 65:7 66:14
110:15 111:1
112:12 116:17
117:3,5

separated 110:16

separately 117:9

September 169:19

series 120:18

serious 36:2 74:5
162:10

serve 92:21

servers 165:21

serves 16:12

service 8:12 16:11
38:11

services 7:9 8:21
11:2 17:1 96:2

session 3:5 6:14
7:3 23:17

sessions 6:9

setting 132:16
142:14

seven 27:1,6

several 15:18
41:16 60:7 118:2
132:14 133:17

169:5

SGML 74:10

shake 10:4

Shapiro 15:16

shared 165:10

sharing 98:19

sharpen 160:13

SHAW-256 50:8

shelf 41:17 86:19

shop 28:21 169:3

short 9:7 38:16
66:15 148:11,21

shortly 40:6

showing 100:3
130:10 166:3

shown 147:6

Shuler 11:8 58:15
60:4 77:9,16
81:6,14 92:3,6
142:6 144:18
145:9

Shuler's 80:19

sibling 116:15,20

sides 51:4

sign 5:20 29:9
36:22 37:5 44:16
53:20 56:17
61:17 82:5,6,12
83:18 85:22
106:16 120:21
124:7 127:6,7
131:17 134:21
140:20 156:11
162:13,14,21,22
167:19 168:4,7

signature 19:11
20:19 43:4

44:1,16 45:4
48:21 49:8 50:11
51:20 52:18 53:5
56:5,16,19
57:3,13 58:7
62:20,21 71:11
83:7 86:4 88:15
91:16,19 97:8
100:4,9 102:3
109:3,4,5,8,18,2
0,22 110:6,14,16
111:5 112:3,15
113:20 114:7,10
116:9,15,20,22
128:3,10,20
134:18 135:3
156:16 165:19

signatures 13:15
22:15 27:16
42:13 43:2,5
51:9 52:14
53:15,20 54:4,15
61:6 62:1 71:8
84:12 86:13 91:3
93:3 96:18
108:17,19,20
109:8,17 110:14
111:18 112:7,18
113:5,7,10
117:17 118:17
135:7

signature's 91:20

signed 5:14,17,21
20:18 38:20
39:10 42:18
74:19 78:21
82:9,17,21
109:13,19
110:8,13,17
111:12 116:21
123:13
124:11,13

127:5,10,12
129:10,16 131:4
151:11
159:10,12
160:4,7,8
161:11,15
162:19
163:2,6,14 168:9

signer 131:15

signers 37:17,21
38:3,8 113:11,14
128:12

significant 63:16
64:14 141:19

significantly 81:9

signing 22:12,14
38:11 42:16,19
56:6 83:19
101:18 106:6
108:16 117:18
120:13,22
128:9,13,17
130:8 163:3

signs 37:18 127:11

silence 138:18

similar 45:13,14
74:6 79:20
171:4,5,10

Similarly 118:4

simple 25:4 97:7
126:5

simpler 25:7

simplest 113:8

simplicity 25:11

simplify 116:5

simplistic 50:4

simply 81:12
115:11 140:9

151:18

Simpson's 97:5

single 75:22 97:8

sir 112:9 142:5
156:4 158:5
162:7

site 145:7 159:21

sites 13:10

sitting 96:19

situation 101:17

situational 92:8

situations 101:18
102:12

situation's 98:15

six 4:18 5:9

size 67:12 140:2
148:10

slice 150:1

sliced 6:17

slices 69:20

slide 18:14 44:3
48:15,16
49:13,21 104:3,7
105:15 108:9,21
149:16 150:3
155:16

slides 3:20 44:10
108:10,15
168:19 169:4,12

slight 34:6

slipped 134:19

slow 72:2

slows 51:8

small 67:6 168:13

smaller 155:12

smallest 166:15

smart 109:21

Smith 5:1 136:21

smooth 119:1

snippet 161:5,6
163:4,6

snippets 14:7

social 142:14
172:10

socially 142:11

Society 10:14,17
66:7 79:17 96:15

software 20:22
21:1 36:14 53:11
59:6 109:21
110:4 114:11
117:4 118:2

solution 6:17
67:11 142:21,22

solutions 5:19 6:22
75:8 148:6,17

solve 6:13 95:11

solved 34:15 40:17
143:2,3,6

solves 53:7

somebody 21:20
32:17 58:3
80:4,7 90:20
94:5 99:17 100:5
122:8 127:6,7
154:12 161:1
166:3

somebody's 54:18
140:15 158:17

somehow 49:11
50:18 82:14,20
134:19,20

141:22

someone 61:4 66:9
69:18 117:3
126:21 127:11
132:2 134:21
153:15 162:10

somewhere 34:6
90:12 110:20
133:7

sooner 169:20

sorry 28:8 47:20
136:17 138:19
162:16

sort 11:12 30:2,20
34:13 36:14
39:4,5 55:19
59:7 66:10
91:4,5 101:13
110:5 131:17
132:17 133:4
147:9 163:19
171:16 172:18

sorts 79:18 107:9

sot 109:5

sound 60:22 103:9
151:12 162:5

sounded 160:12

sounds 102:19
121:10 149:2
162:6 165:4

source 22:20,21
27:7,8 33:12
52:6 53:1,18
54:3
57:5,8,10,11
58:14 59:15,19
65:15 84:14
93:19,20 94:4
100:11,12
123:12 143:18

161:16 165:12

sources 99:7

space 15:1 54:12 58:3 70:7,9,14 120:12 172:4

spaces 154:6

span 30:21

spark 75:20

sparked 44:14

speak 17:6 63:13 65:19 98:3 127:1 163:15

SPEAKER 55:15 103:20

speaking 20:14 39:8 92:6 138:4

speaks 38:2 113:12

special 68:20

Specialist 16:15

specialists 35:18

specific 20:19 26:15 83:13 84:7 90:4 108:5 123:4 145:4 156:11

specifically 61:8

specification 107:14 112:16 113:21,22 116:11 119:5 171:2

specifications 27:15 116:7

speed 67:1

spend 17:16 18:9 149:21

spent 161:19

spin 142:19

Spinning 142:7

spirit 66:22

spoke 33:10

spotlight 74:13

SSL 90:19

St 1:13

staff 12:15 14:14

stages 171:7

stakeholder 18:16 21:10 123:21

stakeholders 48:6

stand 12:11 139:3

standard 20:21,22 21:6 46:3,4,5 58:2 104:18,20 107:11 111:5 112:18 115:9,13 116:11,22 122:4,5,10,14 132:15

standards 8:9 17:15,17 19:18,22 24:18 36:5 46:9,12 51:6 54:8,10,11 99:10 107:11 115:7 116:7 121:3,19,22 122:7 125:15 147:16

standards-creating 115:14

standpoint 60:10,12 127:19 128:22 135:2

Stanford 11:15

36:1 55:18 91:12 97:21

start 15:21 25:17 36:21 43:8 61:13 63:5 68:1 71:5 72:7,15 75:11 86:18 87:3,4 105:5 110:22 114:8,12,13,22 133:19 136:8 147:4,21 155:11 160:13 164:12

started 2:9 3:5 4:7 13:14 17:4 22:6,9,11 101:18,19

starting 16:17 120:11

starts 111:2 118:20 128:2

state 2:18 9:9,15 10:16,19 17:7 28:6 41:9,15 63:12 66:10,11 67:17 83:10 88:7 115:6 131:14 140:11

stated 46:10

statement 134:8 149:4 151:11

States 1:6 65:6,10,12,13

status 7:18

statute 150:18 151:1,9,19

statutes 65:11

statutory 65:4

stenotypy 174:7

step 3:20 22:1 85:6

91:21 110:19 131:12 150:9,16,21 151:5,8

Stephen 116:1

steps 23:22 33:20 133:19

Steve 9:8 41:8 63:7 65:2 88:6 94:1 115:5 140:5 166:17

Steven 5:1 88:3 166:9

Steven's 163:20

stewardship 78:17

sticky 27:9

stimulate 125:12 126:11

stop 25:22

storage 71:4

store 117:17,18,19,20

stored 31:2 56:4

story 6:11

straight 2:10 120:1

straight-through 114:20

strange 61:1

streamline 126:21

strict 143:8

string 164:10

strong 24:1 129:18 135:7,16

structure 70:2 156:4 160:4

161:11,15,18 163:14

structured 170:17

struggled 168:10

struggling 94:18 135:14 145:13

student 8:4 11:16

stuff 42:17 58:19 61:5 77:12 85:20 86:19 110:13 136:6 139:13 141:4

subject 11:12 164:17

subjects 27:22

submit 162:11

submitted 64:3

subsection 168:1

subset 57:3

subsets 5:20

sub-slices 149:18

substantially 36:7

substantiated 131:1 132:7,10

substantive 97:12

subsumed 91:15

subtle 53:19

successful 146:16

succinctly 100:3

sue 80:7

suggest 41:22 65:19

suggested 98:16

suggestion 141:21

suggests 81:8

summarize 113:1 119:11 121:13 122:16 169:6

summary 169:6

summation 122:9

super 122:15 137:20

superintendent 12:2,22 41:2 128:15 130:15

supplier 6:10

suppliers 133:18 148:5

supply 52:8 132:18 159:18

support 5:2 7:4,11 16:15 20:4 49:16 50:16 52:6,7 118:4 159:8 170:16

supporting 49:10 107:15

supportive 95:2

supports 23:12 46:2

suppose 63:10 162:15,18

supposed 11:12

supposedly 92:10

sure 5:15 27:11 29:2,8 30:2 37:7,10 41:10,18 42:11 43:6,14 47:21 55:4,11 64:7,15 78:8 83:10,18 94:4 99:3 101:6 102:9

111:6 122:16 123:22 127:13 129:5 133:3,8 137:6 141:4 146:6 149:3 150:19 158:19

surety 111:22

surprised 131:21

sustainability 68:10

Suzanne 7:5 93:13 126:12,14 136:10,11 143:12,15 144:2

Suzanne's 135:20

Swiatek 16:14

swimming 34:13

switch 26:9 85:15 122:22

sworn 174:6

synced 146:10

synched 33:21

synthesize 72:11 161:5

system 5:9,11 7:13 10:10 13:17 18:18 22:13 32:15 35:3,19 39:5 42:5 64:3 73:12,19 74:1 76:1,8,9,15,16,1 7,18,19,21 78:13 79:8,9,13,14 87:22 90:8 91:4,6 99:8,12 100:14,15,20 101:9 129:13 144:5,9,10 150:22 151:1,5

154:8

systems 19:4 68:14 82:1 111:20 144:11 148:6

system-to-system 105:4 107:2 120:2 144:8

T

table 4:21 49:14,21 50:3

tail 41:13 45:4

taking 6:7 56:17 64:11 69:20 74:9 76:9 90:3 132:8 161:7 168:22

talk 4:3 14:3 28:2 42:15 43:15 44:22 49:22 50:6 54:9 84:2 85:2,19 106:21 108:10,15,20 113:8 136:18 144:8 152:1 160:19 170:7

talked 25:19 44:4 48:18 49:20 52:21 75:21 83:13 86:15 103:6 106:7 123:11 153:1 157:15 170:1 172:1

talking 18:7 21:11 34:21 37:4 43:11 45:15 55:13 66:9 67:19 68:8 92:10 93:2,4,5 94:1 99:5 101:14 105:5 116:13 128:9 138:3

139:8 147:4 153:3 167:16

tangible 18:10 40:16 53:1 63:5

Taoultsides 10:7

target 145:21

targeting 36:3,4,8,12

Task 10:19

tasks 149:11

tax 163:5

team 21:14

teams 21:12

tech 137:14

techies 88:19

technical 6:9 19:4 40:7 78:11 84:19 92:9 105:14 114:17 116:18 118:11 119:15 120:13,19 123:10 137:2 142:10 146:1 148:6

technically 104:11

technique 24:3,4,10 25:3,5,13 49:6 51:11 56:19 57:1,2 81:7

techniques 19:19,22 24:1,8,12,17,20 25:7 27:21 30:13 44:11 45:20 49:8,15,18 50:2,8,11 52:12 56:5,17 57:10,13

70:22 72:19 76:11 96:8 113:15,19 123:10 125:17 147:3

technological 75:8 97:18 142:21

technologically 29:1

technologies 72:22 95:17 127:14

technology 8:9 14:15 44:17 51:16 70:3 77:22 105:7 145:15

Ted 7:8 136:10

Ted's 103:18

ten 2:21 48:17 147:4

tend 49:15 102:14 111:7 146:11

tent 3:15

term 10:16 41:13 51:15,17 57:17,20 60:8 63:11 66:9,12,15,16,18 68:12 70:2 138:5 145:11

terminal 135:3

terminology 43:15 58:2 116:11

terms 7:11 9:21 13:12 18:13 27:3 28:19 29:3 33:11 34:14 39:3 41:3,4 42:1,16 43:15 47:2 64:14 67:18 68:8 72:20

73:2,16 89:19 94:22 96:1 99:5 100:14 130:14 134:16 140:2 156:3 158:6 167:5

terribly 120:15

tertiary 80:4 81:17

testimony 174:5,6

Texas 7:6 93:14 126:15 136:12

text 65:8,9 104:12,13 150:5,22 151:3,12,18 154:9 156:21 160:8,17,18 164:7,10 165:8

thank 4:7 5:5 7:2,21 10:6 12:5 14:11 26:8 32:17 42:7 48:1 58:4 66:21 72:4 94:14 96:13 112:21 118:11 121:11 122:8 137:21 138:15 142:4 153:21 157:13 168:20 170:9

thanks 2:2,6 7:13 28:3 46:18 48:2,15 64:21 70:15 75:18 93:12 95:18 98:17,18,19 103:13,16 104:5 108:7 115:22 117:10 118:9 119:8 121:6 126:13 132:7 134:3 135:17

136:10 156:19 158:4 164:21 172:22

that?s 135:21

that's 4:22 17:17,22 19:11 20:7,19,21 21:14,16,17,22 22:2 23:9,15 24:6,9,14,19,22 25:13,16 26:5 29:18 30:7,15 32:12 33:22 34:7,22 35:21 36:20 37:3 38:4,12 39:19,20 40:2,8 44:9 45:1 46:8,13 48:4 51:3 53:13 54:4 55:6 56:1,20 57:6,8,11,15,20,21,22 58:3,4,9,11,13,21 64:12 66:20 67:4,7,21,22 69:9 70:13,15 71:12 72:14 73:11 74:1,2,9,10,14,18 76:1 77:14 80:6 81:2,20 82:22 83:8,9 85:7,8 86:19 87:6,11,21 88:14,16,22 89:6,16 91:4,11 93:11 94:14 95:1,18,19 96:6,11 97:2 99:22 101:5 102:13 103:1 105:1,22 108:2,5,7,11

110:1,10,13
111:19
112:20,21
114:5,15
115:2,16,20,22
116:19,21
117:5,12 118:9
119:7,8 120:5,16
121:11 122:6
123:13 125:19
127:16
128:13,14,21
129:12,16
130:12,16,17
131:19
132:6,10,11,22
135:4,5,17 136:3
137:4,13,20,21
138:15,20
139:5,7,20
141:7,13 142:4
144:10
145:12,19
149:12 153:22
155:9,14
156:16,19
157:3,5,11,16
158:4,20
159:6,15
161:8,9,17,21
163:2,10,13,15,2
2 164:6,11,14
165:14,16,22
166:1,4,12,13
167:15
168:6,8,9,12,13
169:8 170:5,22
171:21

themselves 29:22
35:21 49:19
51:18 52:5 54:5
165:12

theoretically

167:19

thereafter 174:7

therefore 30:12
65:15 111:7
143:19

there's 3:19 9:22
18:20 19:20
20:1,6 21:8 22:3
37:1 39:7 40:12
42:19 43:17
50:17,21 53:2
64:12 65:3
67:11,16 74:1
76:16 79:4 81:11
85:17 87:1 89:10
97:15,16 98:3
104:20 105:17
110:17 112:16
118:1 128:6
131:4 132:3
133:3,9 141:21
142:3 145:17
152:10 156:2
158:11 159:1
167:17 169:13
170:10,20
172:4,14

they'll 35:5 46:6
69:2

they're 3:20,21
10:22 35:15 36:6
42:16 47:11
51:10 59:8 60:16
61:21 68:18
85:10 88:20
92:9,10
93:16,17,18
94:11,12 102:5,9
104:21 110:18
112:2,3,13
117:2,17,21
120:19 131:1

134:21
136:14,15 137:9
150:2,17
155:18,19
157:19,21

they've 3:15

third 27:9,12 32:9
50:17,20,22
80:14 138:13
153:17

third-party 106:10

**ThisIsAMadeUp
Mashup.com**
98:14

THOMAS 8:18
11:7 15:3

THOMAS.loc.gov
8:13

thoughts 4:6 17:19
19:21 26:4 51:4
75:10 77:6 88:2
98:18 126:12
135:19 146:18
168:16 169:11

threat 71:2
134:12,16
140:22

throughout 64:20
146:8

throw 125:12

thumbprint 50:9

thumbs 118:8

thunder 6:7

tied 13:1 108:4
144:22

till 54:19 72:3
103:12

tilt 118:4

Tim 8:20 9:9 45:2

timeframe 30:19
166:11

tiny 167:6

tired 168:17

title 131:5

titles 7:20 84:16

today 2:3,6,13
5:13,20,22 12:15
13:18 14:16
17:11 18:5,9
19:1,6 20:11
27:11,22 40:9
44:22 50:6,11
55:6 58:11 60:3
67:22 78:19 85:3
103:2 104:3
111:18 121:15
123:11 132:10
147:1 148:20
157:15 169:4

today's 7:22 23:17
37:3 40:13 70:16
81:21 83:1 87:7

tool 143:3

tools 5:13 78:11
91:7 110:4
112:15 119:16
142:10

top 26:9 41:7
47:1,18 50:13
52:13 55:20
158:11

topic 33:13 38:2
43:18 45:15 48:1
53:18 72:11
103:18,21 125:3
126:11 138:18
148:20 157:15

topics 4:2 18:6 19:6 26:11,15 40:8 132:17 171:22 172:7

total 73:15

totally 85:9 95:2,14

tough 156:21 157:1 158:14 168:13

towards 25:10 71:6 162:1

trace 80:5

tracing 13:22 80:16

track 3:18

tracking 9:11 138:13

tradeoff 91:2

traditional 105:10

traditionally 80:20

traditions 77:17 81:10

transcriber 2:13 3:16

transcriber's 42:10

transcript 169:4

transcription 2:20

transfer 76:15,16,17

transferred 90:7

transient 68:10

transit 82:11

transmission 71:4

97:19 144:13

transparency 142:2

travel 125:22

travels 126:3

Treasury 133:12

treaties 65:14

trees 62:2

trial 97:6

trick 67:5

tricky 58:2 86:14,18 87:1 128:8 154:4 166:4,5

tried 21:20 50:4 87:16 146:3 149:7

tries 54:7 113:1

trivial 107:19 133:15

trouble 91:18

true 174:8

trust 28:15 32:4 35:17 50:20 52:4 94:10 98:5 131:15 136:14 144:11

trusted 50:17 143:18

trusting 98:6,8

try 9:14 44:10 48:12 50:15 58:10 61:16 70:3 75:19 87:7,18 96:7 112:22 113:14,22 115:22 117:11

121:14 122:17 126:11 135:5 146:19 150:11 151:5 168:2 169:6

trying 22:22 23:20 46:17 48:11 58:12 72:11 84:22 89:7 92:21 93:2 113:19 115:18 116:5 120:19 140:3 149:17 150:5 154:12,13 163:19 166:2

turn 17:6 72:10 94:17

turned 3:15

turning 165:2,3

turns 24:4 109:15

tweak 102:8

tying 68:9

type 17:21 41:22 42:3 64:16 88:8 105:19 121:3 141:15,22 144:11 155:17 159:10 171:4,5,6

types 5:16 22:4 49:3 65:22 69:22 84:12 86:12 104:9,12 108:19 139:9

typewriting 174:7

———————
U
———————

U.S 63:19 85:22 132:1

UFR 74:21

ultimate 32:5 95:16

ultimately 6:22 7:12 120:5

unambiguous 105:11

unauthenticated 158:18

unchanged 60:11

undergrad 56:16

underneath 109:20

understand 6:1 43:11 69:1 77:10 124:21 127:13 137:3

understanding 43:9

understood 52:17

undertook 132:14 133:17

unfortunately 3:8 78:18

Uniform 10:19

unique 61:8,14,17,19 62:12,14,17 63:2 68:9,19,21 69:3,19 70:17

unit 7:9,10 12:3

United 1:6 65:6,10,12,13

University 7:5 8:4,22 11:8 58:15 77:9 92:3 93:13 126:14 136:11 142:6

unless 77:22 106:2

unofficial 90:1

unofficially 82:10

unreliable 30:4

unsaid 139:7

unsigned 109:13 110:9,12,18 111:13

update 117:10

uploaded 82:16

upon 56:21 73:9 75:5 76:11 117:13 124:5

upper 114:1

ups 3:10 111:1

URL 35:2 56:11 61:9,19 62:10,16 68:9 69:8,11,12 160:9 165:3,7,10,20 169:3

URLs 34:16 68:11,15,19,21 70:3,8,9,17

URNs 68:17

usable 74:2

usage 64:9,20 115:8

useful 72:8 75:21 76:10 81:2,13 85:2,10 87:8,21 92:2 103:9 109:15 149:13,22 150:16 151:14 161:22 164:3,9,13,17

usefulness 92:1

user 13:10 28:14 29:21 32:11 46:6 47:9 48:9 53:12 73:6,21 74:2,13 75:4,16,22 76:16,18,20,21 80:4,13,21 86:5 91:4,16,17 98:2,3 100:15 101:16 102:11 106:7,10 117:15 137:2,16 151:8 153:7 155:17 156:3 158:16 160:2 161:3,4,12,14,15 ,16 167:20

user/consumer 76:2

users 14:5 21:18 23:9 29:18 53:11 58:17 60:1 71:8 77:4 79:14 92:6 93:3,15 94:9 97:22 99:22 101:15,19 106:15,22 107:1 111:14 120:2 136:13 146:11 161:19

user's 150:16

usual 103:19

usually 83:8 118:21

utilization 8:19

utilize 148:2

V

valid 24:3 56:3

136:15

validate 56:7 115:22 120:21 125:15

validation 54:13 55:14,18,21 56:22 57:7,9 63:8 70:12 106:19 109:11 146:14

valuable 24:14,15 49:9 108:14 125:20 160:20

value 6:2,19 18:22 21:16 22:22 46:16 89:11 102:20 114:13 123:19 145:12 152:14,16 153:2 157:5,19 160:12 166:5

value-add 151:22

Vance-Cooks 16:1

variety 97:9

various 16:6 18:15 91:5 99:7 121:8 129:19 132:17 165:1

vary 49:17

verifiable 95:15

verification 57:18 58:19 67:3 70:12 91:8 109:12

verified 60:6

verifiers 37:18,19 38:9

verifies 33:6 138:5

verify 153:10

version 8:13 9:18 13:12,13 31:21 32:3 33:2,3,5,15 35:11 47:5,7 65:11,16 69:16 73:8,9 74:4,15,19,20 78:22 79:3,4 82:7 83:14,16,17 84:15 89:14 90:13 102:6,10 129:9 136:22 138:6 144:2 153:10 158:17

versions 21:19 139:10

versus 43:6 53:21 67:1,2 75:22 99:6 130:5

vetted 93:19

view 38:19 49:4 64:21 77:21 107:12 125:13 136:2 143:8 149:8 151:18

viewers 110:11

viewpoint 75:22 112:22

viewpoints 48:5 98:19 134:1 146:17

virtually 67:18

visual 31:4

vital 144:20

vocabulary 116:22

VOICE 3:13

voicing 115:17

volume 17:15 67:1

105:4 167:10

vouch 143:20

vulnerabilities
134:17

―――――――――
W
―――――――――

W3C 112:17
116:14,22
120:17

wade 155:20

wait 2:17 54:19

walk 103:3

WALSH 154:16

warehouse 62:13

warn 45:3 118:13

Wash 5:4 16:20
78:14 79:4 83:13
111:17,22
112:4,7
170:9,14,19,22
172:14

Washington 1:14

wasn't 28:20 29:2
57:7 157:10
164:17

wastes 24:6

watch 72:1

waves 68:20

ways 19:20 20:2
40:14 44:15
55:3,5 69:21
78:8 83:10
104:20 106:21
108:16 111:3
113:5,16 123:9
130:7,19 143:6
145:4 149:20
153:19 155:21

167:9

WC3 121:19
122:4,14

weak 24:4

web 36:9 69:20
74:12 109:2
146:8 165:3

Weber 11:5

webmaster 15:16

webpage 46:6

website 4:11 58:20
69:18 86:22
90:19,20
94:21,22 134:7
150:12 153:17

websites 34:1
146:5

we'd 4:2 17:18
18:15 19:20 20:7
24:11,14 26:2
72:9 105:12
124:1 126:10
157:5 164:15

week 2:21

weight 87:20
89:10 128:19

weird 42:2 43:1

welcome 2:2,5
14:16 88:20

we'll 2:16,19,22
3:1,3,4,20
4:7,10,22 13:18
17:3,10,11,20
18:3 19:3,13
20:10 31:7 40:17
44:21 45:12 48:3
50:1 54:9
55:4,11,12
58:3,10 71:17

77:8
103:2,8,12,18
104:3 108:20
116:2 117:10
148:15 168:18
169:3,14 172:15

we're 3:9 12:16
13:7 14:10 16:17
17:16
18:1,6,12,17
19:17 20:17
21:15 23:17,19
25:9 27:17
29:15,16 31:4
36:4 37:3 39:8
42:14 43:11,14
44:13
45:18,19,20
46:9,11 48:11
55:7 59:11,14
60:19 67:18
68:17 71:3,13,21
72:6 73:5
77:21,22 78:6
81:7,12 82:9
84:2 86:1,3,4,7
89:7,22 93:22
94:3,6,12,18
95:8,11,17
98:8,21 99:7
102:17 103:2,15
105:1,16,19
106:1 108:12
113:8 114:12
116:13 119:22
121:15
122:16,22
123:20 124:18
133:11 135:14
136:3 138:3
139:8,20 140:3
145:12 148:19
151:21

154:11,13
155:17 160:16
163:18 167:16
169:2,5,18 171:3
172:22

West 153:8 158:19

we've 5:8,18 9:13
12:9 14:18,20
15:8 17:12 18:8
21:9 22:10 29:12
40:16 46:13
48:18 75:20 79:5
85:16,21
86:10,14 94:10
96:10 99:12,18
101:14 106:15
133:14 155:2
157:15 170:21
172:10

whatever 41:19
61:7
64:3,5,16,17
97:7 104:13
138:5 140:19
141:12 142:11
158:10 161:5,6
164:13 168:7
169:14

whenever 74:17

whereas 91:5
108:3 118:15
139:15

Whereupon 173:1

wherever 32:11

whether 13:3
32:6,7,8 33:1
34:4 36:19 37:2
45:8 51:3 59:10
72:14 80:6 97:22
98:12 112:11

134:15 153:16

White 39:10,22 40:9 78:18

whoever 97:14 129:11 165:14

whole 31:11 32:15 97:8 110:2 141:22 167:19,21

whom 174:3

who's 38:21 39:16 52:9 53:18 62:21 66:9 75:1 76:20 80:4 92:11 99:13 131:15 154:12

whose 174:5

widely 122:2

widespread 118:3

widest 87:12

willing 19:9 82:18 83:18 155:19 160:18 162:13,21

win/win 66:5

wireless 3:8

wish 109:2 116:12 168:17

witness 174:5

wondering 36:19 37:2

wording 105:10 164:7

work 5:1 6:9 7:9 8:11,12 10:9,10,15 11:6,18 13:21 15:1,18 16:4,8,10,16,20,

22 24:8 30:11 47:18 54:8 102:17 118:16 136:21 157:6 166:12

worked 15:1,12 70:19 80:17 86:9

workflow 82:14,17 96:1

working 3:9 4:18 5:8 8:6,18 9:10 11:3 12:14 14:22 15:3 21:11 22:11 27:18 63:12 85:13 92:11 106:4 142:1,20 146:2 157:22 169:6 170:15 171:12,15,17

works 24:13 119:1

workshop 1:9 2:3 14:17 45:13 46:17 70:16 96:7 122:18 139:21 173:2

workshops 4:13

world 23:4 31:18 40:13,14,16 50:12 53:1 81:13 85:1,3 88:8,16 95:5,9 102:15 105:17 113:6 121:17 135:7 138:3 139:18 141:9 142:21 144:1,17 153:15 161:1

worried 44:4

worry 126:10 136:6

worth 162:6

worthy 45:5

wrap 18:3

wrapper 97:18 106:13

wrapping 168:19

write 20:22 21:1 80:8 107:18

writing 55:8 59:13

written 41:3

wrong 58:9 85:15 89:9,16 110:13

X

Xerox 170:19

XML 11:13 15:5,14 16:16 19:16,18 28:1 54:10 73:14 74:9 79:4,7 80:12 83:14,16 84:4 104:12 105:5,9,16,19 107:15,17,21 108:10,13,17 112:18 113:6 114:3,20 116:6,19 120:12,22 121:16,21 122:4,10 125:21 160:7

XMLs 108:15

XML's 105:21

XR519 41:1

Y

Y2K 30:22

yet 3:9 27:2,17 83:18 104:20 111:6 122:16 157:16 160:3 169:17,18

you'll 2:17,18 17:6 26:15,20 104:4 118:16 145:16

young 10:3

you've 26:7 34:5 62:4 84:18,19 90:8 97:8 100:3 107:5 108:4 111:3,4 113:3 119:20 144:10 158:21 159:13 162:13

Yu 8:3 36:18 38:10 43:13 58:6 82:3 83:12 90:15 112:10 119:14 131:12 133:2,6 134:3

Z
---

zero 135:8,9

Zwaard 10:9 28:4,8,10