>> Steve Toporoff: Well, welcome again. I hope

state longitudinal databases. And these are intended to be on-the-ground guidance about the nuts and bolts of privacy. The first is on concepts and definitions. The second is about data stewardship, access controls, and issues like that. The third is sort of heavy lifting, and it's about statistical disclosure limitation -- how to be careful when you publish tables that you're not identifying individual students with small cell si

understand that some institutions have decided to forego designating directory information -- some school systems -- because they are afraid that directory information could be used by direct marketers, identity thieves, to be targeted for media campaigns -- whatever. And not having a directory-information policy can be highly problematic for schools, not the least of which because it can render the school district ineligible for certain programs that we administer at the Department. We want schools to have directory-information policies and to communicate with parents about what uses they are making of student data. One large urban school system, for example, wanted to participate in a pilot project that we had that was intended to increase student aid opportunities for low-income students. And we all know sometimes high-school students need a little bit of prodding to prepare their paperwork for college.

school districts will use this change as a pretext to limit legitimate media interest and to engage in viewpoint discrimination. And some commenters, of course, object to the entire notion of directory information. I'd like to mention one more aspect for this discussion, which is student loans. In getting ready for today's presentation, I talked to our inspector general, and we maintain several pages on the Department of Education Website -- the inspector general does -- relating to fraud involving student loans. And so I was interested in that and called her to talk about it. And you have to understand -- the Department of Education doesn't just make grants to states. We also make loans and grants directly to students. I've heard conflicting numbers. I've been told we're the sixth largest and, also, the third largest lender in the United States. Dick probably knows better than I do, anyway. But we're large lenders.

>> Richard Boyle: You're about to be the largest.

>> Kathleen Styles: There we go. And RIG has a large and substantial trade in stopping fraud in student lending. And some of the fraud that occurs is -- it does not involve identity theft. It involves criminal rings that set up groups of people who aren't really going to go to school and getting student loans on their behalf, but a substantial portion does involve identity theft. These, again, like the situations described this morning, are not short-term schemes, where these thieves will use fraudulently obtained Social Security numbers to get credit cards and go to the mall. Hundreds of thousands of dollars are involved, and the fraud can often go on for years. We heard earlier today about child identity theft happening in the family, and we also see that in the student-loan context, as well. I have -- not aware of that before taking this job and before coming here today, and to me, that's the saddest part. It's not unusual for a family member, even a parent, to fraudulently obtain student loans on their child's behalf. Again, we do prosecute. My understanding is, actually, the level of fraud in student-loan lending through identity theft has gone down, that the colleges and universities are becoming more proactive about, you know, helping sniff it out a little earlier in the process. So, I'd just like to wrap up by saying I'm new to Education. I'm so happy to be here today, and I would like us to help be part of the solution to this problem. So, with that...

>> Steve Toporoff: Thank you. Our... [Applause] Moving from the federal level to the state level, our next speaker is Michael Borkoski, who is the technology officer for the Howard County, Maryland, Public School System. Mike.

>> Michael Borkoski: Good afternoon. Before -- I guess, going back, in over 21 years in I.T., since back in the old collegiate days, seen a lot of changes. And the one thing that, over the last several years, has become major has been the amount and abundance of data that is available out there. So, in local school systems, we suffer with that, as well. Howard County Public Schools has over 51,000 students currently enrolled at 73 locations. And these locations, a lot of the times, are looked at as the little red schoolhouse. So -- But we are, in Howard County, a $660 million-a-year corporation, the largest em

afternoon, late-afternoon programs -- folks use our school sometimes. It's our students, teachers doing extracurricular classes -- could be community. It could be the Recreation & Parks area doing something. It could be an event like this being held, as well. We have many people who come in and out of our buildings every day. Most school systems -- and I can definitely speak for Howard County -- we do not have security guards sitting in the front, like out here today, where you would get -- you know, you would have to present your I.D. You have to go through some sort of a monitoring system, maybe even a pat-down. We don't have that. So, our schools -- you can walk in. A lot of times, during the day, you can get to just about any classroom. So the physical side of this is very important, making sure that doors to classrooms, when they're not being used, are locked, because if teachers leave information on the desk, like their grade book, or you know, leave the computer logged on to the e-mail system or whatever, that has to be communicated, as well as at nighttime. A lot of our schools are used for extracurricular activities, like playing basketball or the Boy Scouts or so on and so forth. So our custodians, a lot of times, are in cleaning areas. They'll prop doors open so they don't have to keep using keys. A lot of this comes back to education, education, education. And we talked about it today. I've heard folks talk about it on the side. You cannot have enough awareness. You cannot have enough education around a lot of these issues. A lot of times, when people come into school systems, they want it to be like their home. They want to take their laptop out. They want to go and get onto our wireless network and have access. The problem is, is that network is the same network that houses data that's related to students and even to staff. So a major challenge in the I.T. arena in school systems is to be able to provide the services that are required by the folks that use our buildings, but, also, at the same time, safeguard it. And I always -- I always joke around with my staff, saying we have over 51,000 of the best hackers that come to our work every day. I don't know too many other people that have that. So -- And we have to keep up constantly with changes in technology, the mobile world. We're all still not ready for it. And in education, you know, devices like the Kindles, the iPads, you know, the iPod touches are creating huge challenges because, at the same time where we want to be able to provide access for our students and for our staff, we have to make sure we do it in a very secure way. The last thing, as far as challenges we have in Howard County, and some districts suffer this, as well, is we have a very diverse population. So trying to get folks to understand, who are not of this culture, who did not -- who were not raised or educated in the United States -- to get them to understand that they need to protect their children's information, so -- and they need to be

advocating for their children. So what are we doing to address a lot of these issues? Again, I mentioned a lot about physical security -- worked a lot with and still work a lot with our facilities director in Howard County to just get the awareness out, so that when our custodians walk out of a room, they lock the door. We're putting a lot more badge systems in so we can actually tell who goes in and where and sometimes even question why. We have changed a lot of our policies, and we've actually -- for the first time two years ago, we created a technology security policy for the

engaged in your child's life, not only just from a technology standpoint -- in their life. And as a parent of two children -- and I will tell you my wife is better than I at this, but she knows all their friends. She knows what they do. She also knows online, you know, what their presence is. I remember my son went out and created a Facebook account, and he was 12 years old and went and did it. And you know, he created under someone else's name. So we sat down with him, we talked to him about it and the implications of it, and even to this day, at 14 years old, he doesn't want to touch Facebook. But that's kind of extreme. But at the same time, we sat down and explained all the things that could go wrong with that, even though it was innocent. So -- Because he actually created under a name of a friend of his in class, which was the wrong thing to do. So it tells you that anybody -- and I'm sitting here today as a technology executive in the school system -- it could happen to any of us, so keep that line of communication open with your kids. Reiterate to your children, as well, and, also, parents, please, understand the importance of personal privacy. When you go out and you look out on Twitter, and Twitter is a very good tool to get information out, as well as Facebook, MobileMe -- whatever -- you know, all the different things that are out there -- understand what you're putting out there. You know, as mentioned earlier today, if you have, you know, the location of where someone was born, the city and state, and then you have the last four digits of the Social Security number, if you know what you're doing, you could figure out who that person is. And I knew that before today, because I actually had a guy who works on staff, who worked for the Department of Justice, who actually did it. He did it to me. And it was pretty easy, actually. So, again, and err on the side of caution, as far as, you know, what you're putting out there. You know, if you don't think it's right, don't do it. You know, make sure that you're dealing with trusted sites if you're online, and, also, the requesters that are requesting information, like any telemarketer or anybody else that would call you, know who you're giving your information to. Finally, parents lead by example, you know, so your kids are watching you. And I see that every single day as a leader in the school system -- how the children emulate what they see. Whether it's on television, whether it's live and in person, we are role models, and they are watching us all the time. So, with that, thank you. [Applause]

>> Steve Toporoff: Thanks, Michael. Our next speaker is Larry Wong, who is the supervisor for information assurance and risk management for the Montgomery County, Maryland, Public School System.

>> Larry Wong: Well, thank you for inviting me and allowing me to participate today. Michael, in Montgomery County Public Schools, would be my boss, so he's equivalent to my boss. And what -- The work I do is information security. I had a lot of names in the past -- I.T. security officer, information officer, data officer. The most common one everyone calls me is "The Hammer" because I say no -- "You can't -- You can't do this. You can't do that," and there are reasons behind that. Well, in any security program, it has to come top down. And I always have the conversation -- with Denny -- Denny earlier and, also, Michael -- we were talking about how, anytime you want to implement a program, if you don't have support from top down, from management on down, if they don't buy into it, if they don't believe in it, if they don't see that there's an importance to have that security program, then no matter how hard I work and no matter how many times I go buy this technology or buy that technology or talk to this group of people or talk to that group of staff, it's not gonna make a difference. It has to come from top down. And one thing that we've had in Montgomery County is we've had that top-down support. And the way is -- that you can see it is Montgomery County Public Schools, along with the Department of Police, Montgomery County Department of Police, and, also, with the Montgomery County State's Attorney's Office -- we formed a partnership. Now, in that partnership, we -- together we crafted a message, a cybersafety message and cyberbullying message, and we're working on other messages, as well, that goes into the cyberethics. Because Montgomery -- the University of Maryland has a C-3 Conference they have every year, and they call it "Cybersafety, Cyberbullying, and Cyberethics." And we're kind of starting to adopt that model. And of course, included in that cyberethics piece is the identity theft, copyright, stealing intellectual property -- all those things that are underneath that cyberethics piece. So we have this comprehensive program where three agencies are working together side by side, and we have the same message, and it also gives us an advantage. Earlier, when I was listening to some of the conversation in the previous panels where they're talking about foster care or other situations, when you don't -- if you don't know who to call -- For instance, when -- in our school system, if I have a situation where I haven't experienced it before, it's very easy because I have that partnership -- pick up the phone, call the police at the Family Crimes Unit, say, "I have this experience going on. What do I do? "I have a parent that called me on the hotline. What do I do?" "I received an e-mail through the cybersafety e-mail system, and they said they're experiencing this. What do I do?" If the police can't answer me, I take up the next phone -- I called

-- the phone again and call the cyber -- the State's Attorney's Office. "Hey, we're experiencing this. What's your advice?" And so we have this. Montgomery County police and Montgomery County School District has a memorandum about understanding -- if this happens, we do this. If that happens, they do that. You know, we share information. We work together, and we're partners. So that's -- I think that's a unique thing. When I talk to my peers across the state and perhaps across the country, there's not -- I don't hear a lot of these collaboration groups, where these partnerships exist. And so I would think that that is a very key thing for success. It's been very successful for us because we've had some major events, and by having those relationships it made the process easier. In the news a couple -- back in 2010 -- January 2010, we had a large data-loss event, where we had some grades changed. And the grade-changing event occurred because we -- every school district and every corporation and perhaps all families across the nation is experiencing this increase, influxes so quick of data, technology and things -- devices coming at you. I mean, you're -- you can't even -- by the time you buy the first iPad, the second iPad's knocking at the door, and if you buy the first Android device, there's three more behind it, so you can't keep up. Well, what happened was, there was a device that allowed students -- and allows anyone -- to steal information. And so information was stolen, and then we had a large data breach. Well, this cooperation, this partnership we had -- as soon as the event happened was -- I started my initial investigation, and then I got to say, "Okay, this is a lot bigger than I thought it should -- it's gonna be," and then I make a phone call to the police. The police gets involved. The next thing you know, we get the State's Attorneys involved. And so then, we're able -- as a group, we're able to then take this situation and then manage it in the way it needed to be managed. And because we -- what has happened is, it's not a matter of if you're gonna have a data-loss event -- it's a matter of when you're gonna have a data-loss event. And when you have that data-loss event, you have to be ready. You have to be ready. You got to know what you're gonna do. Step one, who do we call? Step one -- Step two, what do you do? -- step by step by step. And Montgomery County Schools has just recently gone through the Malcolm Baldrige process. And understanding and having a process, you know who to call, what to do, when to do it, when to throw your hands up and say, "It's time to bring other people involved," into your situation -- that's very key to the success of

or, recently, Massachusetts had that tornado that landed in that town, you got to think about, "If that happens, what will we do as an -- for the emergency?" So you got to plan way ahead. And that's one thing we have done, and we've been successful. We're able to, if any data-loss event occurs, we're able to respond to it pretty quickly, identify it. We have systems. We have system loggers, where we can capture all of our data, so that we can then go back and then trace it through some forensics, you know, investigation and identify what happened when, who did it, and so forth. So we have a lot of that in place. So -- So, mainly I just wanted to share was the fact that we have that top-down management support and we have this collaboration. And you know, when you have a data-loss event, you just got to be able to take it -- as you hit the ground, just run with it and get it -- and get it taken care of, because I don't like being in the news. I don't like my name published in the news -- nothing like that. My boss -- If Michael was my boss, he'd be like, "Larry, why are we on the news?" No, we're gonna do our best to try to keep that down. The other thing, too, is, we have to keep -- understand that there's a lot of technology available out there and it's coming really quick. And the folks who are creating this technology -- they're not security-minded. So, sometimes, it's very difficult for Michael, myself, and other school districts to get our arms around it. So, right now 'cause I'm -- we're trying to figure out, "How do we integrate all these new devices into our network? How do I let the mom or the contractor or the child bring their device inside our schools?" And those are challenges that we have. So, having those cooperations, having those pre-established procedures, and then forward thinking about, you know, playing that movie, so to speak, 'cause as soon as you -- as soon as someone brings that next, new, I don't know, Android Mega Monster device into your school, how are you gonna deal with it? You got to start thinking about that early, and that's what I wanted to share this afternoon. Thanks. [Applause]

>> Steve Toporoff: Thanks, Larry. Well, our next speaker is Richard Boyle, and he is the president and C.E.O. of ECMC Group. And he's going to give us some insight into what his company has learned in connection with a data breach of student-loan information. Richard?

>> Richard Boyle: Yeah, thank you very much, Steven. Thank you very much for being part of the audience. I would like to dispel the thought process that maybe C.E.O.s are on the ball, because

organization. And if there's anyone in this room -- to go back to what Larry said -- I will put my full salary -- which is not substantial, but it's not bad -- my full next year's salary on anyone in this room who thinks this cannot happen to you. It can happen to you. And as I walk through my organization and I find PII data, even today, in an unguarded situation, I just cringe because it says to me that we have to go back and strengthen the training and the culture of our firm. And so I defy anyone to think it's not going to happen to you, because it will. Stay diligent -- physical and data security controls must be continuously improved and changed -- again, your point, Larry, and your point, Michael. Know where your data is and ensure that it is secure. P.C.s and laptops -- for example, our laptops, while they were encrypted, our hard drives could easily be taken. Some of the -- It takes about 30 minutes for someone to come into your facility and take the hard drive out of your computer. 30 -- 30 minutes? -- 30 seconds. Excuse me -- 30 seconds. Your laptops -- you want all your laptops to be encoded, definitely 256-bit encryption -- definitely. You want to be able, on all your iPads, to be able to wipe the iPads. If somebody takes them, wipe them. I have the little -- I carry the iPhone. This iPhone can be sort of like Mr. Phelps -- totally wiped clean. We can wipe clean any one of the programs or all of them on it. In fact, my guys know exactly where I'm at -- every iPhone -- we follow in the U.S. We're in all 50 states and the principalities. Know what's in your filing cabinets. Know how many filing cabinets you have. Know how many safes you have and why do you have safes in your organization. Know what kind of portable media you have. And why do you have portable media at all? If you are dealing in PII situations, you should not have it. And then, finally, understand your systems. On policies, your policies must be easy to understand, and your policies can't just be at the senior level -- they must be accessible to everyone in the organization. We badge in, and we badge out. If you don't badge out, you can't badge back in. We have guards. We don't -- not quite this difficult, but you can't get through our organization. We don't give out free water, so I better be careful here. You don't get free water at the Department of Ed, by the way -- that's my regulator. Know what -- who comes into your building. Question everyone. Now, I'm the C.E.O. I'm a very, very happy guy, and I'm very, very happy with my people. And I'll walk in, I'll open up the door, and I'll invite them all in. That happens once. Now, they stop, each person has to badge in, and they'll lecture me on security. That's what you want. That's the culture that you want. You have to continually remind people, you have to be training for employees. You have to enhance, You have to train, You have to test, and you have to audit -- every single one of those steps -- and you never tire of doing any of it. Or

Keep them constantly on the knowledge base so that they know that your whole company reputation is at stake,

Wall Street" -- I train in "The Wall Street Journal" for my folks, and then I immediately have a training in security. And I also give money to people who stop security -- potential security breaches or identify it out of my own pocket. And if you -- if I find that you have PII on your desk, I take your computer, I take the PII, and you come and see me personally. If it happens three times, I fire you. You are gone. It's a company policy. Only had to do it once, and I did it, unfortunately, to a highly valuable employee. But if nobody -- nobody -- me, a board member, no one is going to abrogate the responsibility to PII and to protecting our confidential information for our borrowers, and we will never put our reputation

identity is, is really important. Larry also wanted me to make some observations about what we're seeing. Because we, you know -- It's really interesting. And I know the Department of Education will bear out on this, and that is that the real estate in the classroom is filled up. The time is full. And when you go to a school and you need to say, "Well, now, you need to be teaching identity

in the classroom. It has to be activity-based. So when you look for an education program, whether it's on identity or any other e-safety thing, you're going to want to make sure that that curriculum, if the schools are at all interested in it, is that kind of a curriculum. One other thing I wanted to mention, and this ties in to this issue of critical infrastructure and data loss. It is an issue that you've experienced now, but I think a great number of people are going to experience it in the future. It's coming. And one of you said it before. If you haven't experienced it yet, you know, it's a question of when. As a result of that, insurance companies have been coming to us -- one in particular in California, Keenan & Associates -- and they insure schools for liability -- all kinds of different liability. And they said, "You know what's going to really come and get us and get our schools and we're going to be playing a lot of claims out on it, it's going to be loss of critical infrastructure and data. And so what we want to do is we want -- we want to retain you, i-SAFE, to take your education into the schools in California that we insure. And we're going to help you, okay, persuade those schools that they need to be teaching this to these youngsters in K, pre-K, all the way through the 12th grade, be teaching the teachers on how to protect this information, putting it into their acceptable use policies, et cetera. And then, of course, obviously, if they decide not to do it, we can decide later on when there's that data breach whether or not we're going to pay that claim. But it's an interesting development that you see that's coming, where insurance companies are coming to us to help us get our program on Internet safety into the schools. Okay? But it is on this issue of data -- critical infrastructure and data loss that they're really concerned about. So, with that, I just wanted to share with you those two issues. One, look for that data-loss and critical-infrastructure problems to increase, and, two, I just wanted to stress the fact that we've got a lot of work to do yet in terms of getting the kinds of education that we do into the schools. It's difficult, okay? It's just going to take time, and we're going to have to figure out how to integrate it into that very, very tight space that's available, or unavailable, to the schools. But we're making progress.

>> Steve Toporoff: Well, thank you. Thanks. [Applause] Wanted to thank all the panelists today. We don't really have time for questions, but we're on break, so if you do have questions, I'm sure the panelists wouldn't mind taking a few minutes to speak with you. So, thanks.