Kristen LaFave: First, I'd like to welcome you all to Session Number 57: Low Cost Tips to Improve Student Data Security and Privacy. My name is Kristen LaFave, and I'm a senior privacy specialist with the Department of Education in our privacy safeguards office, and our panelists today – I'm going to go ahead and introduce them now. First, we have Chuck Tobler, who is the privacy advocate for federal student aide. In that role, he oversees all compliance and reach response activities for FSA, educates the FSA and partner community about privacy issues, helps incorporate privacy concern into business and technology decisions.

He has more than ten years of experience in information assurance in privacy and has worked for numerous federal agencies as well as in the private sector. He has a masters degree in public policy from George Mason University, and he's a certified information systems security professional and a certified information privacy professional. And speaking about security today is Ross Hughes. Again, he's with federal student aide. He's the cyber security manager with more than 39 years of experience in telecommunications, information security, and cyber security. His background includes work with DOD, NSA, local and state governments, various commercial organizations, and he currently manages a team of cyber security analysts and engineers who are tasked with identifying, tracking, and protecting against computer threats to federal student aide systems and data.

He carries many security and audit certifications and a BS in information security management from the University of Maryland and Baltimore County. So again, thank you for joining us today. We're really excited to talk about our favorite topics, security and privacy, and I'm going to see if I can figure out my slide presentation. Voila. Okay, so we just wanted to take a few minutes before we get started on the meat of the presentation to talk to you a little bit about some of the recent privacy initiatives at the Department of Education. We have a lot going on. We're very excited to talk to you all about it.

First, we have a new CPO and a reorganized program office. We have a new privacy technical assistance center, the PTAC. We have some interesting technical briefs we released, and of course, we have our notice of proposed rule making for FERPA. Now first, when I say we have a new chief privacy officer, I don't just mean we hired somebody new. I mean also, we have established an office of the chief privacy officer, and that's new for Ed, and it's really exciting. Her name is Kathleen Styles, and she comes to us from the Census Bureau.

She's a lawyer and a certified privacy professional, and we're really excited to have her on board to run the privacy office. When we hired her, we reorganized our entire information management offices, and so now – whoops, I went ahead, didn't I? Sorry. We hired her. She's going to be handling FOYA, privacy safeguards, information clearance, records and documents management, and also, we've brought over the FERPA team, the FPCO, under her as well. So we're all going to be working together to do all of the privacy and information management under the office of management, which is the chief privacy officers' office. Now why did Ed establish this position?

Well, when privacy first started gaining prominence in the last few years, privacy was usually handled by like OGC or FOYA or IT or – you know, it was put in all kinds of really crazy places, and it was never really a good fit. Privacy is its own discipline. It's got its own policies, and it's really well complimentary, and there's a lot of overlap with these other offices. It really needed to be its own office. So Ed realized that, like most other federal agencies right now, and established this office, and I think it's really going to – she's got a lot of great ideas, and she's really excited to be here, and I think she's got a lot of good initiatives that she's going to be rolling out in the next couple years.

The second initiative I wanted to talk about was the PTAC. This was initially intended sort of as a one-stop resource for education stakeholders to learn about privacy, security, and different ways to approach that. It was initially focused on longitudinal data systems grantees. Now it's broader. For those of you who don't know what this, it's simply a way that people can study students and student-achievement in schools over many years, and of course, there's a lot of privacy issues involved with that, so they established the PTAC. I keep hitting this button, and I apologize.

So now that we're trying to broaden the focus from just longitudinal data studies to something more. So what we're doing is providing technical assistance to states and other education stakeholders. Mostly things that don't fall neatly under FERPA. Most of you know about FERPA, and there's things that aren't found under FERPA, so this is somewhere people can go for that. It's going to be disseminating updated information, best practices, et cetera. I've got the website up here, and you guys will be able to get that. You can also simply go the Ed site and Google it. It's very simple to find.

If you go to that website, you're going to find this privacy toolkit, and again, it's going to have FAQs, documents of interest, best practices, and it's really relevant not just to these people studying education statistics, but really, for all people with stakeholders, education stakeholders. There's going to be training materials. There's some great presentations and webinars, things I think you'll really find interesting.

One of the things you'll find there are these technical briefs. Again, these are intended initially to assist with the state longitudinal data studies, but again, we're really trying to broaden the scope. We put these out for comments, so if you want to take a look at some of the ones in draft and give us comments, we're very appreciative of any input you want to give us. There are currently three available. Basic concepts and definitions of privacy and security, I think it's a really good document, really gives you some background. There's one on data stewardship, and then statistical methods for data protection.

But again, we're going to be rolling out a bunch more of these over the next year or two, and I hope you'll take a look because I think you'll find it really useful. So now, I always want to talk about the elephant in the room, and that's the FERPA rules that have come out. In April, we issued a notice of proposed rulemaking. The comments closed in May. We got almost 300 comments. Some of them were wildly supportive. Some were wildly opposed. We got a real gamut of comments, but they were all very helpful. We reviewed all of them, considered all of them. Some of you may have had folks in your schools who commented, and we really appreciate all the comments that we got.

I guess what I can say about is the timeline, and I think this was intended to be the end of the calendar year. We were going to issue the final regs by the end of the calendar year, and as you can see, we're coming up on that in the very near future, considering December 1st is this week. So I think you can expect to see the rules very soon. And if you're interested in sort of keeping track of that, finding out when they come up, we have a list serve, and there's other ways to find that out, so feel free to come talk to me afterwards about that, or just go ahead and go to the website. If you can go to http://www.Ed.gov and search for FERPA, you'll find the website and how to get involved with all that stuff.

And needless to say, I can't speculate on what's going to be in the final reg, but you know, certainly it'll be out soon, and you guys can all take a look for yourself. So those are the big privacy

initiatives that have happened over the last year. And one final thing I wanted to talk about just briefly was privacy incidents. You know, this is a big issue. There's an organization called The Privacy Rights Clearing House, and I put up some statistics. What they do is they track reported incidents over the years and try to get an understanding of where the reaches are, what's the causes, and they track by government, by education, by corporations, different groups, and you can really do a search and sort of target what you're looking for. So I did a search by educational institutions, and this is what I came up with.

Now it kind of looks like, "Hey, we've had fewer this year. This is great." But I gotta say that I think it's very deceptive. I think part of the problem is breaches are vastly under reported, and also, there's no real consistent reporting requirements. Like what is a privacy breach? If you e-mailed somebody an e-mail with Social Security number in that without encryption, are they going to report that? Good Lord. Are they going to report that, and is that going to come up in these statistics or not? So it's kind of hard to figure out how that works, but you know, I do want to point out that there were 53 breaches reported, and that's almost 400,000 – well, 390,000 records, and that's a lot of records. So I think that this is something we all need to be concerned about.

It's especially a problem for institutions such as colleges because colleges particularly are a real target for cyber security criminals because the problem is you guys have so much data, and there's such big turnover. You've got Social Security numbers and financial information and education information. And not just for students, but employees and their – the parents of students, and it's just ripe with all this data, and there's so much turnover. You're getting new students every year. And the other issue is by your very nature, you're a place that wants open access and open learning and sharing of information, and because of that, some of the systems are – have security vulnerabilities that a lot of other organizations might not have.

So you've got this ripe target. You've got maybe some security issues. So I think that it's really important to know that you guys are probably prime targets for cyber criminals. And I think this is a real problem because of the great costs of the breaches. And I'm not just talking about money, which s a huge issue, but you know, reputation. I mean it gets in the press and it's really embarrassing when your school has lost data like that. Also, people won't trust you, and you might hurt your recruiting or whatever. The costs of money are significant. The Ponemon Institute is an institute that

studies this. And they found that in 2010, a cost of an incident was 200 per compromised record, and $7.2 million per event. I mean this is a huge amount of money in a budget-cramped school. So it's something to really be aware of. And the reason that I chose this slide to be last was it's the perfect segue to have me pitch it over to these guys who are going to talk about how to prevent these kind of breaches from happening. So at that, I am going to go ahead and – I actually am going to hold questions or comments until the very end, so I'm going to let Chuck go and Ross go, and then we'll have a question and answer session. So thank you very much, and here is Chuck.

Chuck Tobler: Good morning. Thank you, Kristen, for the introduction. Thank you everyone for coming out. I'm really excited to be here. It's my first conference, so if I make a few mistakes, you can blame it on being a new guy. I guess the flipside is if I do well, it's just beginner's luck. So normally, I ask can everyone hear me, but for the folks way back there in the other zip code, can everyone see me? Because I am here. Okay. Last joke. I know I'm the last thing standing in between you guys and lunch, so I'm not going to sit up here and bore you with a bunch of Power Point slides and a long speech.

I'm actually very efficient. I'm going to do it with just a few slides and a short speech, I mean. So you'll notice up here we say privacy is everybody's business. Before we begin, I'd like to just kind of define privacy. There's actually a lot of different types of privacy, but when I'm talking about privacy today, I'm talking about information privacy, and that's basically controlling the information about you that is released. And you'll the word PII a lot. That's kind of a government term. It stands for personally identifiable information.

So it's information that can be used to uniquely identify someone. Your classic is like your name and your Social Security number, driver's license number, credit card information. So what do we mean by low cost tips? That is the focus. I'm going to have to put this down for a second. Excuse me. I'll start off with one example. Every year, Verizon releases a data breach report, and it's done in conjunction with the US Secret Service and the Dutch High Tech Crimes Unit. It's a great report. It's fairly technical, but one stat that is not technical at all that really stands out is they said that in 2010, 96 percent of data breaches were preventable by simple or intermediate measures.

So what do I mean by a simple measure? When most hackers steal data, they steal it form servers. So when you buy a server, put some software on it, generally that software enables you to apply a password and password protect your servers. So there's low-cost tip number one. Please password protect your servers and actually use a strong password. And Ross is actually going to show you how easy it is to create a strong password that's also easy to memorize. So there's first tip number one.

Now did everyone get the super tippy top-secret paper? And if you did not, could you please raise your hands? Okay, could we come up and please – oh, Kristen can do it. Thank you. Who already turned the paper over? Okay, that's okay. Actually, that marking kind of highlights that there's a debate in the community whether should you mark sensitive documents as sensitive or should you not. Some people say we shouldn't because if you do, then the thieves know, "Hey, sensitive data here." But other people say, "No," because right people want to do the right thing, and you need to tell them, "Hey, this is sensitive data." I'm on the side of I think you should mark it, by the way, but there are people that think you shouldn't. Okay, could you now flip the paper over?

And yes, I know, a test already. But hey, we're the Department of Education. We like our standardized tests. But I would like for you all to just take a few minutes and read through these questions. You don't need to write down your answers or anything like that, but it's actually a really short but very useful test. I give this one out a lot, so just take a few minutes. I'll stop talking and go through and answer the questions. Do we need a few more minutes, or has everyone had the chance to at least look through all the questions?

Okay, well, what you just did was actually conduct what high priced consultants like to call a gap analysis, and I know because I used to be a high-priced consultant for Deloitte. So I really do like this test, though, because one of the main benefits is it really helps you to identify your strengths and your vulnerabilities, and the importance of that is it allows you to focus your resources. Because you know, let's face it. We don't have unlimited budgets. And as you see, you don't have to higher an expensive consultant.

And for those of you who want even more pain, Ross actually helped develop a very detailed self-assessment that we'd be happy to share with you. Done correctly, a self-assessment is really a valuable tool. Another thing that's really nice about them, I'm sure we've all been through audits and we know how pleasant that

is. Auditors like metrics, and a self-assessment is a really good metric that you can show to an auditor. "Hey, yes, we do take security and privacy seriously." I'm sorry, these slides keep jumping ahead and I don't know what's going on. So that's another reason is it's a very – this is very jumpy.

Anyway, so it's a very good metric. Okay, now I'm going to kind of move on to the meat of the presentation. So first things first, know thyself. And everything I'm going to tell you – actually, these slides are out of order. I'm sorry. Okay, everything I'm going to tell you today basically falls into one of four categories, and the first is establish good governance. Second is know what you know. Third is reduce your exposure, and four is remember, privacy is more than just the IT department. This is something I'll probably repeat several times. I can even distill that a little further and say basically in three words bake it in. What I mean is a privacy by design, build privacy into all of your business decisions and your technical processes, and make privacy everybody's business, as ironic as that sounds.

That's really what you want to do. Okay, so tip number one is establish good governance. First thing you really need to do is create policies and procedures. They really are the foundation of any security and privacy program. You know, building a privacy program without policies and procedures is equivalent to building a house without a blueprint. People want to do the right thing, but actually, you need to tell them what the right thing is. Don't assume that people know what the right thing is. So it is important.

I'd say two more things about policies is one, don't make them shelf ware, and two, don't make them door stops. And what I mean by that is shelf ware, you need to update your policies regularly, take a look at them at least annually. Don't make them doorstops. Don't have your policy document be, you know, five inches thick and weigh ten pounds. Keep them clear and concise. That way you'll know that people will read them and actually, more importantly, understand them. Second is identify a privacy official.

It doesn't necessarily have to be a full-time job, but definitely someone that's sort of a point person for questions related to privacy. And one of the main things about this, again, relating to it's more than just the IT department. Not that IT is not important. It's very important. But make sure privacy has a seat at the table. Business decisions, technical decisions, that type of thing. And

last, budget analysts or program analysts are often kind of a good bridge between privacy and the more technical sides of the house. Okay, training and awareness. I really cannot overemphasize the importance of training. There's a lot of good, free training available. We have some links to some free training at the end.

Of course, we'd be happy to work with you to develop custom training programs, but there's an old joke in the security field that if we can only get rid of users, our systems would be secure. So you really have to focus on your users. Crooks are clever, and they're also very opportunistic, so they kind of get it that we're getting better at sort of what I call boundary protection with technology like firewalls and intrusion detection systems and things like this. So they go for the weak part, and that's often the user through the classic phishing e-mail attack or malware on a website. "Hey, we have this great offer. Click here."

And boom. Then the virus is in. So I like to call it the human firewall, and again, this kind of relates to making privacy everybody's business. Publisher rules of behavior. Rules of behavior is basically a very short document, one or two pages, that kind of spells out the rules of the road before you give someone access to your system. You know, things like don't share your password, report security incidents, lock up your laptop. That type of thing. Don't look at data you're not supposed to look at. Last, you know, unfortunately, breaches do happen as Kristen pointed out.

They are sort of unavoidable. So the key is you really need to have a plan. You know, the last thing you want is it's a slow news day. There's been a breach, and the media is calling, and you don't have a plan. You're sitting there at the press conference kind of winging it. That's the last thing you want. So take some time and develop a plan. Roles, responsibilities, how to report an incident, how to identify an incident, who calls who, who calls who and when, how do we escalate, do we notify? Make sure you fulfill all of your notification requirements. I believe there are 46 separate state data breach notification laws. I actually suggest that you read them because they're actually pretty helpful.

They sort of spell out very clearly what you need to do. And also, a question I get a lot, which my answer is usually it depends is what is PII. The state laws really spell it out. If you have name and combination with this, this, and this, you have to report it. So they actually do answer some questions. Okay, so is there a corollary to know thyself? Yes, it is, and it is know what you

know. What do I mean by this? Do you really know how much PII or sensitive data that you have? Were you collected? What are the entry points? Where you do you store it? Where does it go? Who touches it? Why do they touch it? Do they really need to touch it? I used to be a technical editor for many years, and my general rule of thumb was without even seeing your manuscript, I can cut it by 10 percent, probably 20 percent. So being that we're in Las Vegas, I would wager a gamble with you that I can take a look at your PII inventory and cut it by ten percent at least. I'll give you an example, which I'll take a step back.

So in editing, and I didn't make this up. An author of an editing book did. They called it the saw, the pruning hook, and the Exacto knife. Okay, so the saw would be take a look at your business process. Do we really need the Social Security number at all, or do we even need this business process at all? Why are we doing this? The pruning hook is okay, we need the process. Maybe it has ten separate sub-processes. Do we really need to share the social for every sub-process? Okay, now you're down to the Exacto knife. Yes, we do. We need it. We need it for all ten sub-processes. Okay. Do we really need to collect it on a form, then enter that into a database then send it to someone via e-mail, put it out on a website? Just looking at ways to reduce your PII exposure.

So that's why mapping out your business process flows, I guarantee you you're going to figure out ways to reduce your exposure, and true story, I was a contractor for a large federal agency who just said up and down we need the Social Security for this process, and absolutely we do, and there's no way you can cut it down. Well, we get to talking, and another tip, we're mapping out the business process flows, and you've got to have not just a high-level program official, but sort of a front line person that actually does the day-to-day work.

And we looked at it, and the program official said, "We don't use the social for that," and the frontline person said, "Yeah, we do, and we send out like 15 million a year via e-mail." So I'm glad I wasn't part of that conversation after I left the room, but the bottom line is just from that one conversation, we got rid of that business process and reduced the exposure by 15 million Social Security numbers a year.

So it is definitely possible. And this kind of relates to tip three, which is reduce your exposure. So there are a few things you can do, and again, reducing your exposure is just limiting the number of places where the data is. I always kind of think of it somewhat

negative, but what could the bad person do? Because you do have to sometimes put on your bad person hat. So think of the places where a bad actor could access your data, or actually, a human could make an error. So one is clean desk. Clean desk policy is pretty simple. It just means, hey, at the end of the day or when you go on break, clear your desk of paper. Put it in a locked filing cabinet. Don't lose that USB drive. Don't leave it on your desk. Put it away.

Second one, I call it PII amnesty days. I'm also willing to bet that in addition to the data you have on your servers, you probably have a lot of employees that have a spreadsheet with 50,000 socials or a database on their hard drive, or maybe they have e-mailed it to their home e-mail account because they want to work from home, and you don't have an EPN so they can do that. So create what I call amnesty days. Like hey, no penalties, but please, sort of turn it in, and let's get rid of it because you do want to create a culture of trust.

Don't feel like you're punishing your employees for doing this, but I think it's a good idea. We actually do a similar thing at Federal Student Aide. It's records management week, and we actually make it kind of fun, believe it or not. We have a contest to see what office can fill up the most shredding bins – secured shredding bins, I might add. So it's kind of a good idea. Okay, data at the end points. This is actually what kind of keeps me up at night. In particular, USB drives. An end point is pretty much any data that's not on a centralized server, so it actually includes paper.

The USB drives, laptops, smart phones. I would say that the key concept here with especially laptops, smart phones, and USB drives is encryption. Encryption is simply scrambling data so that someone can't read it unless they have a password. Ross will show you there's really some good free encryption programs. Encryption is sort of your get out of jail free card when it comes to privacy and particular data breaches. Almost every state law says if the data was encrypted, you don't have to notify. And as Kristen said, notification is expensive. I mean some people say about $214.00 per individual that you notify. So again, encryption is your get out of jail free card.

Again, USB drives scare me because it's just really easy to put a lot of data on them and lose them, and just if you don't actually restrict what drives can be used, just have some good policies in place and educate your users. That's another true story. They're also what we would call a threat vector. There's a lot of viruses on

them, and there's kind of a famous story where they went around the Pentagon parking lot and dropped off about, I don't know, 40 or 50 – a bunch of USB drives, and the number of people that picked them up and stuck them in their computer was frightening. It was like upwards of 80 percent. So just be aware. Okay. You wouldn't know that I work for the technology office. Would you? I cannot get this thing to go forward. I promise there is another slide. Destroy your data securely.

That means shred paper documents. Don't just hit the delete button. That actually does not delete a file. Someone could easily recover it. You need to wipe it clean. There are tools available that are like DOD approved that will literally wipe your data so that it can't be read. You can also shred a disk or burn it if you'd like, but the point is destroy it securely. Do not keep records forever. Ross and I did some site visits this year, and we were surprised at how many people when you asked them, "How long do you keep your records," they say, "Well, forever." I encourage you to – every state has a state records retention policy.

I would encourage you to look at it, and if you can get rid of stuff, I would get rid of it. Last, this is somewhat of a technical one so I'm not going to talk about it too much, but you want to limit access to only those that really have a need to know. It's this is more the logical access control. But the concepts are basically least privilege and separation of duties. So least privilege – only give people access to the minimum amount of information they need to do their job. Role based access, Ross, I think is going to talk about that a little more. Again, that's a little more technical, how you assign privileges to users on information systems.

Practice breach prevention. What do I mean by this? As Kristen said, there are several organizations that track breaches, and we actually have the link to two of them at the end. This is kind of the old saying, "Ounce of prevention is worth a pound of cure." So I would learn form other peoples' mistakes, basically. It's really interesting to kind of go through this database because while it is true that the majority is 50 – I think it's 55 percent were the result of hacking, technical, almost as many were the result of just simple human error. These are good people just making mistakes, basically, because maybe they've not been trained, or maybe you don't have the proper policy in place.

You know, a classic example is e-mailing data to the home account, not getting rid of data that's no longer necessary. Recently, there was a fairly large breach with the state of Texas,

and what they had done was they shut down this system, but they left the web server up with millions and millions of records because basically, someone had forgotten about it, and someone was able to hack in and get it. So again, just kind of think a little bit. And that is why training is so important.

You're probably wondering when do we get to the technology part. So am I ever going to talk about information technology? No. In fact, Ross is going to talk about that. But before I introduce him, again, my last tip, privacy is more in IT department, but IT is very important. But you need to have people, process, and technology. They all need to work together. Once again, I'm going to say bake privacy in. Don't bolt it on. It's also a lot less expensive to build privacy in from the beginning than to bolt it on later. And the Tootsie Roll defense, that's kind of an old security saying. Hard on the outside, soft on the inside. Hard meaning yes, we have firewalls and intrusion detection and all sorts of good technical stuff.

But on the inside, you look at our internal processes, maybe our users were not quite as good. Again, that gets to the importance of training. So another last thing is you can have security without privacy, but you can't have privacy without security. So peaking of security, I'd like to introduce Ross Hughes. Thanks.

Ross Hughes: Thank you, Chuck. Let's see if I can work this. All right. I know things are – Halloween is over, but I couldn't resist extending it a little bit, so I'm going to show you some scary stuff for the tricks, and then later on, I'll give you some treats. So for those of you who have been on Survivor Island for the last 20 years, this is all going to be new. For the rest of you, you've seen it, you've heard it, you've ignored it, so I'm going to hit you over the head with it once again. So we're going to start out with some big numbers.

One hundred and ninety-four million network attacks blocked. Sixty-four million web intrusions prevented. Two hundred and fifty-eight million malicious programs detected and neutralized by one vendor in one month. Now social media is the advertisers' golden child, and it's the second brain for everyone under the age of 40. But it's also one of the main vectors for malicious programs getting into networks now.

We all live by social media. We all have our iPhones. They're all hooked into our networks. And that's the new way that people are hacking into systems. And if you think the latest is the greatest, Google Chrome, 27 or 100 extension on Google Chrome are

vulnerable to attacks. Some more scary stuff. In the federal government, network incidents are up 650 percent in the last five years. Thirty-nine percent just in 2010. Brute force attacks on passwords or iPhones – the iPhones, the smart phones, the tablets, that's the new laptops. Everybody is using them. The android I've got in my pocket, that's the most attacked operating system. We're going to have to live with it, but how do we access them?

We access them with user accounts and passwords. That's why we're really pushing to factor its indication. Because if you'll see here, passwords can easily be cracked. So if you're going to use them, which is one of our tips, you can't afford to factor authentication, go with passwords, but the more, the merrier. The longer, the better. Some of the headlines that I have to live with every day and which is the reason I don't have any hair anymore. Some of the scary ones, SSL certificates for CIA, MI6, and Mossad were hacked. But my favorite is the Facebook blind date.

They met on Facebook. It was love. They decided to have a romantic interlude, so they set up a meeting. When he went to the meeting, he closed his store, rushed to the meeting, and while he was gone, the other person broke into the supermarket and robbed him blind. Love, what can you say? Okay, promise, this is the last one. A hundred and fifty-thousand malware incidences looked at every day. A new web attack every 4.5 seconds. Remember the old joke that on the internet, nobody knows you're a dog? Well, 99.999 percent of the people on the internet, you don't know. So be very careful who you're talking to.

And most of the people surveyed said that they know that social media is the most insecure system. Eighty-one percent say that they know Facebook is the most insecure, but they still use it. So for the budget people, this is probably the scariest slide because this is what it costs. Homeland Security, for their 2011 budget, $614 million. Network security budgets across the industry have increased 11 percent, and the experts say that by 2016, they'll be spending over $10 billion on network security.

So what's that mean to you? What can we do to save you some money? So that's why we're here. So you've had all the tricks. So now, we'll give you some treats. What should you do? The first thing is use what you have. You don't have to buy the latest, the greatest. You don't have to have the newest out there. You have to remember, hardware, software vendors are there to sell you products. It's not us. It's the machine doing it.

Evaluate your threats based on what you've got. Do you really need the $220 million security infrastructure to protect the cafeteria menu? If you've got some secret recipes, maybe, but probably not. So look at your data. As Chuck said, get rid of as much as you can, and then look at your data, look at what you've got, see if you can use that to protect. Leverage your knowledge base. Your computer security department is a good resource.

If you're evaluating a new product, if you're looking at some security technologies that will protect your applications, give them to one of your professors, let him use it as a class project to evaluate in the class, give your report, let you know what's going on. Open source. Open source is our friend. A lot of free stuff out there. A lot of good stuff. A lot of the security products that are out there now started as open source. But remember, not everything is free. So there are maybe some costs involved, such as training, such as you may have to upgrade your hardware. And re-purpose your old hardware.

You don't have to throw everything away. You can put a Linux firewall on an old server. You can use them for storage. There's a lot of things you can do. Hire interns instead of professionals. You could supplement your staff. Hire interns, hire students, but keep an eye on the students. They're slippery. Your training costs might increase. Training time might increase, but I think in the long run, you'll probably save money. Look at your policies and procedures. Are you doing things that you probably can save money on? Is there 25 steps in one of your processes, and you only need five? Can you save the time and the money?

So review your processes, review your procedures, and as an ex-consultant, it pains me to say this, but hire a consultant as a last resort. Use your internal assets first. But when you do need to hire outside assets, it may save you some money in certain places. Save you on training, save you on benefits. They have to keep things up to date. You don't. And evaluate your insurance options. You know, there's three things you can do with risk. You can ignore it and hope it goes away, you can fix it, or you can transfer it. And if you have insurance, that's transferring the risk. Let the insurance company pay for all the breaches, getting everything fixed.

And I threw this last one on here. The umbrella liability insurance. That covered everything else, all the little things. My wife made me get this for our two houses because she said if Santa falls off the roof and I put on the coat, she doesn't want me going to the

North Pole. So the insurance company pays for everything. And as Chuck said, security is not just IT. It's people, technology, operations. We call it the three-legged stool. And if you have to hire consultants, if you have to hire a new security person, don't try to be cheap because security is expensive. People with the experience and the knowledge to help you, they come at a price, but you have to understand that not everything is the purchase price.

It's kind of like real estate. You buy a house, but then you have to also figure in what are the taxes, what are the community costs, where are the schools. So do the comparison because you might have training. You might have to upgrade your servers. And just like real estate, location, location, location. Here is compare, compare, compare. Compare your systems, compare the new technologies, see which one meets your needs at the right price. And as Chuck stated but we're going to state it again, training is very, very important.

A knowledgeable staff is a secure staff. You've had all this squishy stuff, so now we get to some hardcore stuff. Passwords. If you can't afford to factor authentication, then passwords is the way to go. One of the issues we've always had was that passwords have always been weak, and the reason is because people have 15 different systems. They're trying to remember 15 different passwords. And so they make them easy to remember or they add numbers to the end of them. I've been at this for almost 40 years, and I learn something new every day.

And I learn this code system last month, and I think it's really neat. Because you only have to remember a couple things. You start out with picking whatever system you're going to do. Like in this case, it's by bank. So it's your bank website. And then you have a code that bills your password, and it's whatever code you want. In this case, it's capitalize the fourth character, move the second to the last character at the front, add a number, move a – put an alphanumeric character. And then, it dumps out your password, and you can make it any kind of code you want. But all you have to remember is use the same code for every time you want to do a password.

All you have to remember is a different name for every site. Like if you've got http://www.Amazon.com, you feed it into the code. Dumps out your password. Works every time, so all you have to remember is whatever the code is, switching things around, and then whatever you've named your website. PayPal,

http://www.Amazon.com. It's really neat. You can make it as long as you want. Come up with any code you want. Switch things around. You can have a 16, 15-letter code, and it comes up with a password, you only have to remember that I'm doing this, and whatever I call the password. The other things is phrases.

I use phrases all the time. Favorite song, your verse, a book. In this case, you need eight characters, and a special character. So I've got Snow White and the Seven Dwarfs. Eight characters, plus SM, Superman. Special character. Change them often. Every 90 days. Don't make it too short because then people won't want to remember it. They won't memorize it. "Why do that? I'll just write it down." So keep it around 90 days, which is fine. Encryption. Chuck mentioned encryption. WinZip, pretty much the industry standard. Not that expensive. It's like weighed encryption, but it works.

There's a lot of open source encryption products out there. I use one called J-Zip, which is a very, very good product. Okay. Session locks. Another thing that's very important, you don't want the password sitting up on the screen while somebody goes to lunch, so make sure that your desktops have session locks where the system will lock itself down. They have to log back in. For your applications, it's really based on what you're doing . You're doing a lot of batch processing. Of course, your session locks have to be fairly long. And awareness.

Along with training comes awareness. The posters. You've got to keep security on everyone's radar. You can't say, "Okay, I trained all my people last year. They're good to go for 12 months." It doesn't work that way. You can't put people on automatic. Security has got to be constant. My first computer instructor back in the day when tablets were made of stone used to say, "You can't fix stupid." Well, it's true. People are always going to be your weakest link. So you've got to keep them trained. You've got to keep them aware. It used to be it's easy to find the Phishing e-mails because they had misspellings, the logos looked wrong, they all came from Nigeria, offered you $100 million.

Nowadays, they look just like your bank's website. They look like they came from PayPal. So the only way you can do it is keep your users suspicious. If it looks too good to be true, it is. Knowledge is power. Constant e-mails, newsletters. Keep security out there. Open source. Open source is our friend. We've got some *Cyber Security for Dummies* books up here free. Come get them. Also, I've got a handout. It's probably the best

free security list in the world. This is one of my favorite sites. If you print this out, it's over 102 pages long. So there's a link, and there's also a link in the presentation. Go to the site and look at it because it's 102 pages of links to free software, to scanners, anti-virus programs. Everything is free. So look at it, evaluate it. This may be one of your better resources to actually look at things.

Training. You can get training from vendors for free, training on the internet for free. Linux has a lot of free firewalls. Just do your research. If you use the internet, remember the dog. So be leery of who you're talking to on the internet. But policies, the government has a lot of free policies, templates. Sands has the same thing. NSA, DISA. We have a lot of information we can give you on hardening systems. So there's a lot of free resources out there. Use the government as much as possible.

And the last thing I'm going to talk about is physical security, as Chuck talked about it. Lock it, lock it, lock it. Lock your shred bins. Lock your desktops. Lock your wiring closets. And with that, I'm going to turn it back over to Kristen to wrap up us.

Kristen LaFave: Okay. Well are these turned on? Can everybody hear me? Okay because I'm going to go ahead and sit down for this last section. Except I need to move the slide. So thank you, first of all, to Chuck and Ross for giving us this great presentation. Just a couple of things I noticed. From Chuck's section, I really thought his four tips are very useful. Good governance. I particularly liked to have a privacy POC. You don't have to pay to have a chief privacy officer, although that's obviously very nice, but as long as you have someone who is sort of the go-to person for privacy and can keep the knowledge and keep an eye on things, that would be great.

And also, as Chuck pointed out, the time to figure out a plan to respond to a breach is not when the breach happens. It is extremely important to develop a plan in advance, to have a group of people who are going to come together who can figure out what are you going to do, how are you going to notify people, how are you going to talk to the press. There's a lot of free resources out there about how to do a breach response. Particularly in the federal government, and it's very transferrable to other organizations. So that's really important. Another thing was the complete of PII inventory because you cannot protect it if you do not know it exists, and I am telling you right now that there are people in your organization who have PII that you do not know about. There's a lot of ways to go about this.

One thing we did was we just wrote up a survey, a very short survey, and gave it out to all the organizations and said, "Tell us. What kind of PI do you collect? Where do you keep it?" And you can actually do one-on-one interviews with the person, too, and really delve deep and figure out where all the PII is. Again, you guys have lots. Students, their parents, employees, et cetera. So really get in there and talk to your people about where they keep the data. And again, it's not electronic. You have systems, but you also have paper files, and as Chuck pointed out, all the mobile stuff.

So really try to figure out where all that data is. It is not easy. When I first came to Ed and we tried to do this, I thought the CIO had the list of all the PII, but they did not have anything about the paper products, and then a lot of the times, some of the POs or principle offices will go ahead and develop a system without the CIO's help necessarily, and so they don't know about it. Chuck?

Chuck Tobler: Would you mind if – I'm going to put in talking about forms. I've done PII reduction for a lot of organizations. And you usually start with a forms review, and you look at all the forms you have, and I like to call it the save as effect. You're looking at one form, or you don't see why would you need to collect the Social, and you ask the person, and they say, "Well, I don't know." Why is the field there? A lot of times, people have to create a new form. They open an existing form and go, "Save as," and save it as a new filename. Say the Social was legitimately on the first form, but they forgot to delete it from the second one.

So – and I can't tell you how many times this has happened, so people are filling out this form with the social, and there's no need for it. So the paper is _____. Sorry.

Kristen LaFave: Oh, no, please. Any time you guys want to jump in on the conclusion. Also, the reduce your exposure, obviously that's really important. I thought obviously, you don't want to collect anything you don't need, and this bears repeating. People do it on autopilot. It probably was once useful information and it's no longer. Really question people. Do you really need this data? And another thing that I think is vital is do not keep records forever. Because any records that you keep forever are just more that can be hacked, stolen, lost, whatever. And in the federal government, we have the federal records act, and it governs that exactly, and it tells us exactly how long you keep information, when you're allowed to destroy it, and what just needs to be kept forever.

So at least when you have a policy that talks about, "Well, student grades, we have to keep forever, so we're just going to make sure that we put that in a secure location and keep it." Other stuff, registration, classes or whatever, maybe you only need to keep that for a couple years, and then you can destroy it. Of course, destroy it well. Don't just think deleting is going to work. And again, privacy is more than IT. That's a really important part that bears repeating, and it's everybody's business. Everybody needs to get involved with making sure that they understand that this data is valuable to criminals and dangerous if it gets out. People need to sort of a culture of privacy awareness.

And then from the security side – whoops. We went ahead again. Seriously, this slide thing is – go back. So security might entail some costs, but not having security will cost much, much more. And I remind you of my $7.2 million cost of an incident. There was an incident in the education community, not a school, that ended up costing the company $20 million, which is nobody can afford that. Saving money is about making sound decisions on the right products and processes, and I think Ross gave us some really good guidance on that. Security is more than the IT. IT's people, processes, technologies. These are all key components. They have to work together to secure your data.

Privacy and security are everyone's responsibilities. A chain is only as strong as its weakest link. And as we mentioned, the weakest link is people. People are the weakest link. So training, awareness, constantly making sure people know how to treat data. What do you do with it? Can you e-mail PII? Not usually if it's particularly valuable. Do people know how to encrypt stuff? This is something that's important, too. Especially if for example, this comes up a lot, a school will e-mail to the Department of Education a spreadsheet with hundreds of Social Security numbers and names on it. That's technically a breach, even if we don't know that it was seen or stolen from anyone, but that's a policy breach. You're not supposed to do that.

So we really need you all to understand that you can't just e-mail Social Security numbers in the clear. And then finally, we've moved ahead again, but I'll just say that this is Ross saying, "If you have any questions, call Chuck." I think you can call Ross, too, but Chuck is the privacy advocate at FSA. Very knowledgeable about FSA. Very knowledgeable about privacy, and he's happy to answer any questions particular to the FSA folks, and I am happy to talk to anyone about any bigger issues,

any other issues about privacy. You know, I work in the main organization at ED, and we establish a privacy policy within ED, and we are happy to talk to you all about anything.

So anyway, on that note, I think I will go ahead and open it up to questions. We are happy to entertain any questions about privacy, security. There's a microphone right there that I believe is on, or you can just raise your hand and shout at me and I'll just repeat the question. Yeah, hi. Go ahead.

Audience: This is something that wasn't covered, but it's an issue on our campus that we've been talking about a lot. What are your recommendations at the best way to authenticate identity? Someone calls up. How do you know who that person is, who is calling? This is especially true since we've been sort of given guidance from Department of Education that we can't use Social Security number and date of birth to authenticate identity.

Kristen LaFave: Okay, thank you. The question was about authentication of identity. Because they've been given guidance about not using SSNs, which was in the maybe 10 or 15 years ago, that was very common. When someone called, you'd say, "I've got your record. What's your Social Security number," to authenticate that person, and that's really being discouraged nowadays. Ross, do you have any comment on what's a good way to authenticate people? Are you talking particularly about phone, or just any old way?

Audience: Mainly talking about phone and e-mail, also. We get a lot of e-mail. Obviously, we get e-mails from parents.

Kristen LaFave: Is that something – so yeah, phone is big, and other ways, too. So let me ask Ross about that.

Ross Hughes: Yeah, when you're authenticating, you've still got to have something you know or something you have. When you're on the phone, it's got to be something you know. So if you can't use Social Security numbers, in most cases, what people do, it's like the banks. They set up security questions. So if you have a security question, and hopefully it's – we had a presentation yesterday. They said if it asks for the street that you were born on, don't say Main Street. Say, "Street near the oak tree," or something so somebody can't Google you and find out you lived on Main Street. But really, when you're using phone calls, the only way you can authenticate someone if you're not going to use a Social Security number is with security questions.

It's what the banks do. It's really the only easy way to do that, unless everybody in the world has their two factor identification tokens.

Chuck Tobler: A few other things, too. You could maybe only take calls or have people register phone numbers, and they're just sort of authorized phone numbers, and check to see if the call is coming from that phone number. Something that my bank does, which is pretty interesting, is they ask for my address, and then they ask for the nearest cross street, and I would assume – because it's easy to get someone's address. But they say, "Do you really know sort of where you're at? What's the nearest cross street?" And I think, honestly, they just use Google maps to do it.

Kristen LaFave: Feel free to give me your name. We have some help desks, and I know that we do authenticate because people are always asking us for questions, and they call in, and we need to authenticate them. I don't have off the top of my head how we do that, but I can certainly find out how Ed does it, and I'd be happy to share that with you if you wanted to drop me an e-mail. Now I have to go through this whole thing again. Any other questions for Chuck or Ross about security, privacy?

Audience: Yeah. Whoa. Just a quick question. Several years ago at FSA conferences, they were talking about the possibility that the Department of Ed would get away from using Social Security number, and communications with school on the FAFSA and with direct loan, trying to use alternate ID of some kind and get away from that, and certainly, Social Security number on the icer documents and all the direct loan and health originations and documents coming back and forth are where we have the largest usage of it is where our largest needing to keep having Social Security number around.

Is there any idea if there is any movement to move ahead with that in the future, or is that kind of dead?

Kristen LaFave: I can – I'll talk generally, and if Chuck has something to add. First of all, one of the big issues is that we did an analysis of our systems and our forms and how we handle things. And in many cases, we are actually required – I'm sorry. I didn't repeat the question, but I think he was loud enough for everybody to hear. He's asking are we looking towards getting away from using the Social Security number. So frankly, a lot of this financial stuff, we actually have to use the Social Security number. The way the systems are set up, the way we work with other organizations like

the IRS, a lot of this we do have to use the Social Security number. A couple years ago, OMB who is where we take our policy direction from, came out with a directive that said, "Please cut down your usage. Eliminate any unnecessary usage of SSNs." So all the federal government agencies are trying to get away from it, but it's a real challenge because it's a multi- I hate to use the word billion, but it may be up to that much money to change a lot of these existing systems, especially at the Social Security Administration, IRS, us, et cetera.

We are definitely trying to get away from that where we can. But this is again, it's sort of – it's like turning a cruise ship. We already do it like this. We've got all our systems set up like this. Data, you know, moves downstream. And to change one thing, you have to change everything else all the way downstream. So I wish we were moving faster. I wish I could have better news. We are definitely trying to get away from it, but it's not something that's going to happen overnight, and maybe Chuck has something that he can add.

Chuck Tobler: I would just say that on the FAFSA itself, Kristen is right. It's actually really not the department that requires the social, but basically, when a student applies for a student loan, he actually undergoes a background check, and it's run through Homeland Security, Health and Human Services for the deadbeat dad, IRS. So it's a lot of the other agencies that actually require on the initial application. I know that we are, Ross, I think we're looking at re-engineering the PIN process where the students register for a PIN to, I believe, get rid of the Social for the PIN registration.

I think on the FAFSA itself, as Kristen said, it's a big cruise ship. All agencies have been instructed to reduce the use of the SSN, but it's just going to take some time.

Audience: Yeah. Certainly, we couldn't get rid of it, but it's in a large number of places. With our University of Missouri system, we're going through – we're finishing up this year, we're remediating SSN from all of our active databases and using an SSN bolt, and it's a really involved process, and we – when we've been working with our system level folks in the – form the financial aide office, it's been rather painful because we have been in so many places, even like on direct loan, unique IDs for loans, there's SSNs embedded in all of those. Those kinds of things are causing a lot of headaches and hassles. It's just something I was wondering if in the past at conferences, they mentioned they were heading away from that kind of – some SSN from being so prevalent in all of the

documents, so I was just wondering if there was any movement towards that. So thank you.

Chuck Tobler: Actually, I would like to work with you on that. I'd be happy to map that process out, so I'll give you my card, and please feel free to contact me.

Kristen LaFave: Any other questions? Okay, let me slowly go through this the other way. Sorry, one more question. Great, hello.

Audience: I'd like to know since some operating systems are more vulnerable to viruses and spyware than others, does the department have its own preference as far as what operating system it uses on desktops?

Kristen LaFave: Ross.

Ross Hughes: Everything is vulnerable. I don't think there's – you know, we used to say, "You can't hack a Mac." That's no longer true. I don't think there's a system out there right now that's any less vulnerable. If it becomes popular, such as Androids – first, they were hacking iPhones. Androids were okay. Now Androids are becoming more popular. Now Androids are the most hit systems. We try not to make recommendations on what to use for operating systems. I personally like the different flavors of Linux, but for desktops, we have Macs. We have Windows. Windows 7 is getting more and more secure. It's the ubiquitous operating system out there, but I don't think there's any one perfect system out there.

Chuck Tobler: I'd say the main thing is to keep your patches up to date and run scans regularly, too, and have like a standard desktop configuration is very helpful.

Audience: Thank you.

Kristen LaFave: Thank you. I'm just going to show you this. Everyone is going to have access. Everyone at this conference is going to get access to these slides, so you don't have to write down every slide, but Chuck and Ross have put together an amazing list of free resources for privacy, and then Ross had that one slide that gives you a link to all the free resources for security. And here is our contact information. We are delighted to entertain questions, comments, feedback of any sort. We can be your contacts at Ed for privacy and security, so if you have any particular questions or you need us to follow up on something, don't be shy about giving us a call. We just want to thank you all for coming. We're always really excited

to talk about this topic. As you can see, we have a lot of ideas, and we're very passionate about student privacy, and we really want to help you protect your own students. So thank you for coming. Thank you for panelists, Chuck and Ross, and thank you to the folks who helped us out, and have a great lunch.

[End of Audio]