

**THE CENTER FOR STRATEGIC AND INTERNATIONAL
STUDIES**

**“PROTECTING CRITICAL BANKING AND FINANCIAL
SERVICES: ROUNDTABLE SERIES ON PRIVATE SECTOR AVIAN
INFLUENZA PREPAREDNESS.”**

WELCOMING REMARKS:

**ANNE SOLOMON,
SENIOR ADVISOR, TECHNOLOGY AND PUBLIC POLICY, CSIS**

KEYNOTE:

**DONALD F. DONAHUE,
CHARIMAN, FINANCIAL SERVICES SECTOR COORDINATING
COUNCIL FOR CRITICAL INFRASTRUCTURE PROTECTION
AND HOMELAND SECURITY (FSSCC)**

THURSDAY, MARCH, 16TH, 2006

*Transcript by:
Federal News Service
Washington, D.C.*

ANNE SOLOMON: If everybody will take their seats. Get a cup of coffee.

I'd like to welcome all of you. I'm Anne Solomon. I'm a senior advisor at CSIS for technology policy, and we have a great audience here this morning and it's because the reliability of our critical infrastructure in the event of a global avian flu pandemic is now one of the primary concerns in Washington; perhaps not quite as high up on the agenda as Iraq and Iran, but enormously important. I imagine a lot of you saw the business section of the New York Times this morning that had a front page article on avian flu and business preparedness for avian flu. I was pleased to read that the Cartoon Channel will continue to operate throughout a global pandemic, even though other businesses may be crippled by employee absences and transportation communication disruptions.

For the majority of the public, I suppose that continuity of operations and business in banking and financial services primarily means that they will be able to continue to get those \$20 bills out of their ATM machines, but this morning we'll hear from a number of key individuals who are working to ensure business continuity of the critical banking and financial services and who are wrestling with far more complex issues. I'm pleased to introduce our key note speaker, someone whom most of you know who will open discussions. Don Donahue serves as the chairman of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security, which I've learned is usually known as FSSCC. Is that correct?

DONALD DONAHUE: That's right.

MS. SOLOMON: FSSCC. Don also serves as the Chairman of the Partnership for Critical Infrastructure Security, which is the organization of all sector coordinators under Homeland Security Presidential Directive No. 7. In his spare time, Mr. Donahue serves as the chief operating officer for The Depository Trust and Clearing Corporation and as the president and COO of two of the DTCC operating subsidiaries, The Depository Trust Company and the National Securities Clearing Corporation. We very much appreciate his coming down here this morning from New York to keynote these discussions.

Don?

MR. DONAHUE: Thank you, Anne. And thank you all – thank you all for attending this very important session this morning. I got an e-mail from one of my co-panelists, I think somewhere around 7:30 this morning, that said, “Make sure to read the

front page of the business section of the New York Times,” which I did. I actually thought the article that ensued was a whole lot more accurate than the headline was, and hopefully we will convey some of that to you today.

The whole process of preparing the nation for the possibility of an avian flu pandemic is obviously a work in progress for the nation as a whole and it's a work in progress for businesses as a whole and it's a work in progress for the financial sector as well. The fact is that we cannot possibly be at the end point of knowing precisely what all preparations need to be deployed. That is an impossibility today given how many unknowns there are about how a possible pandemic might unfold – it's totally unrealistic at this point to think that anyone would answer the question “Are we fully prepared?” with a “Yes.” But what we are trying to convey this morning – hopefully will very successfully convey this morning – is that the banking and finance sector is very actively moving forward to identify the issues associated with the possibility of a pandemic and to address those issues. And I think you will find that we have a very, very good story to tell along those lines.

In preparation for doing that, I need to give you a few minutes of introduction to the whole infrastructure protection issue, the organizations involved in that issue and how that issue itself has evolved over the last decade. This will really set the stage for talking about how that infrastructure protection effort is now going to be deployed to address the avian flu issue. So I'm going to give you some intro on that as a beginning. I would suspect that there are very, very few people in the room who have ever heard the name FSSCC before, so I think we need to be clear about some of that right at the start.

The national critical infrastructure protection effort has actually been underway since the mid-'90s. It's been underway for a decade now. It is focusing on the reality that there are a number of sectors in the economy and in the society of this nation that are critical components of this nation's ability to continue to function and continue to act in a normal state.

The responsibility for protecting those infrastructures is now currently on an overall basis resting with the Department for Homeland Security. In many of the sectors there is an agency of the government specifically designated with the responsibility for that sector. This slide shows some of the sectors that are identified as critical sectors under this effort. There are actually 17 including the ones that you see on the slide in front of you and they pretty much cover the gamut in terms of the essential services that people need to be able to continue to conduct their lives and the essential services that the economy needs to be able to continue to operate.

Specifically for banking and finance, Treasury – actually very much in the person of Scott Parsons, my co-panelist – has the direct responsibility for monitoring infrastructure protection efforts with respect to the banking and finance sector. Treasury works very closely with a working group known as the Financial and Banking Information Infrastructure Committee, pronounced FBIIC, which is essentially all of the regulators involved in financial services. All of those people will come together in the

form of the FBIIC to talk about and address issues that arise with respect to infrastructure protection.

Critical infrastructure protection is, you know, a very formidable sounding phrase but we need to be very clear about what that means. What is the infrastructure that we're talking about here? What parts of that infrastructure are critical? What do we mean when we say we have to protect the critical infrastructure? What exactly does that entail and who are the parties who actually have to do that? Don't assume that all of those answers are immediately obvious. There are things that really have to be thought through. They are in fact issues that have been very successfully thought through over the 10 years that we'd been focused on this. We have many, many of the answers to them.

I'm not going to spend a whole of time on this but the essential theme here is that each of the components of banking and finance has to be broken down into tiers. In thinking about infrastructure protection, you have to focus on what are the issues with respect to those tiers and how do you protect those tiers? How do you prioritize them? Which are the ones you focus on first? Which are the ones you focus on next? What are the needs each of those tiers has? And how do you go about making sure that the institutions in each of those layers can continue to operate regardless of what the circumstances are? The essential model that you will find in banking and finance – we represent it as a pyramid on this slide, but probably the more useful graphical image is to think of this in terms of rings of concentric circles – is that you have core infrastructures in the sector that handle tasks that must go on whatever the circumstances. These tasks include typically how you handle payments, how you settle financial transactions and how you maintain records with respect to payments and settlements that have occurred.

You have other core infrastructures that set up transactions that that first layer handles, settles, takes care of – the example on the securities side would be the trading markets. Then you have all of the users of those infrastructures and you differentiate among them as well. The most important component in this tier consists of the firms that represent a substantial part of a particular financial market – the rule of thumb is someone who does 5 percent of the activity in a particular market is viewed as being a significant component of that market. Essentially, if you throw a party and that person doesn't show up, you're going to have a problem because that is a serious amount of market involvement that you need to have at the table.

And then you move out into additional layers which are people that collectively represent an important part of a particular financial market, but in their own individual capacities represent a lower transaction volume, represent a lower number of customers, whatever the metric is that you're measuring. And you're saying the infrastructure protection focused on that layer is at a lower level of intensity. The system as a whole could survive that person not being part of – not operating as part of the system for a period of time. And that's the approach we've taken.

This slide illustrates how you do that tiering on the investment side. This slide is how you do the tiering with respect to banks. You have payment systems. You have wholesale payment systems. You have retail payment systems and you have the users of those systems. You have a similar architecture with respect to insurance, as represented on this third slide. Each of these slides represents an intra-sector view.

There is also the very critical issue that each of the national sectors in many serious respects depends on the continued operation of some of the other sectors. The example in banking and finance we always use is that telecommunications is critical for banking and finance. If the telecommunications capability of the nation is knocked out, banking and finance essentially can't operate. Of course, those of you who are familiar with the actual events in banking and finance on September 11th will know that it was a failure of the telecommunications environment that necessitated the trading markets to close for the week. It wasn't the trading markets themselves – they were perfectly able to operate. It was the fact that the telecommunications network in lower Manhattan had been so damaged that people couldn't get orders to the market. That's what caused them to make the decision to close. In other parts of the sector, including the payment and settlement part that I represent, we were able to continue operating without missing a beat during that entire week. So that's a very good illustration of this cross-sector dependency issue that's very relevant here.

The difficulty that infrastructure protection presents, in many respects, is due to the fact that 85 percent or more of the infrastructures that the nation needs to protect in each of these sectors are in private-sector hands. They are not national infrastructures. They are not governmentally owned infrastructures, by and large. They are actually private companies that operate particular key components of the infrastructures, pretty much in all the sectors. So the national plan says we need two instrumentalities to help marshal the private sector to deal with this. We need a sector coordinating council in the sector that addresses the issue on a policy level: what are the key priorities for the sector in proceeding on this effort? And we need what the documents refer to as an information sharing and analysis mechanism, which is how do you communicate within the sector about this issue? How do you send out alerts? How do you send out, you know, information that indicates there's a terrorist threat against certain financial institutions – the issue we faced 18 months ago – how does that information get out to the sector? And you have an information sharing and analysis mechanism that is responsible for doing that.

In banking and finance, those two organizations are the Financial Services Sector Coordinating Council, or FSSCC, which handles the policy setting issues for banking and finance, and the Financial Services Information Sharing and Analysis Center – the FS/ISAC – which handles the information sharing aspects of the responsibility. Both of them operate under the aegis of Treasury and operate very closely with Treasury as our sector-specific agency.

FSSCC is essentially a parallel organization to FBIIC. On this slide, FBIIC is on the left; FSSCC is on the right. FSSCC is composed entirely of private sector

organizations. We have many banking and finance trade associations. We have key banking and finance infrastructures involved in this policy-setting exercise as well. And FSSCC has a number of priorities and a number of initiatives that it has underway to address various components of the infrastructure protection issue with respect to banking and finance. You see them listed on this slide.

We think one of our key responsibilities is to make sure that the world knows what actually is going on. The banking and finance sector has an incredibly impressive story to tell in this space, but if the tree falls in the forest and isn't able to tell people that it fell, nobody knows. So what we've tried to do is also to make very clear how much energy goes into this and what has been accomplished in this phase. And you see illustrated there a copy of an annual report on FSSCC activities in promoting infrastructure protection in 2005 that we issued this week. And we actually are hoping that copies are going to arrive here before the conference ends this morning, so that we could give you copies of the annual report; if not you can see it on the FSSCC website, which is identified on the slide.

As we've implemented all of these instrumentalities to deal with the infrastructure protection issue, the whole concept of infrastructure protection itself has involved over that same time frame. 1998, you know, was the first time I had ever heard the words "infrastructure protection," but banking and finance has been doing continuity of operations since somewhere in the 1300s. Banking and finance has been dealing with business continuity, has been dealing with security issues since the first banks were created. We were doing infrastructure protection even at the time Jesse James did the Great Northfield, Minnesota bank robbery, right?. We just didn't call it that. Infrastructure protection is an issue that we have paid a lot of attention to and have a lot of experience with. But it has really morphed in very significant ways over the last few years and I think that understanding those changes is important when you start talking about how we're going to be addressing the avian flu issue.

If you went back 10 years ago and talked to people about continuity of operations or talked to people about business continuity, you would hear a perspective on that issue that was very location-focused. I operate in this location, if something happens to this building that's the problem I've got to deal with. I have a fire in my data center, how am I going to recover from that? You had a very physical disaster-focused orientation. It was all – it was fires and data centers. That was the kind of thing that people planned for. It was also very common at that point to have the view that I can come back in two days and that's acceptable. A lot of people outsourced business continuity – even in the core components that I described earlier, we relied on outsourced arrangements where we'd go to a disaster recovery vendor and recover in their space a day and a half, two days later, and that was considered state-of-the-art 10 years ago.

The Year 2000 issue, the millennium bug, if you can cast your mind back to that particular delightful exercise we all went through – that was when the whole way people were thinking about business continuity as an issue began to evolve. The Y2K issue drove home very, very clearly that the performance of information technology systems is

critical to the ability of banking and finance to operate. Y2K, of course, was a cyber issue; it wasn't a physical issue. Y2K also really underscored the network issue – that if I'm fine but my counterpart is not able to operate, there's no point in me being fine. We began to understand that the sector functions as a network and the health of the network and the health of each other was a critical part of the business continuity strategy that every organization had to be focused on.

One of the things you saw evolving in banking and finance as a result of this is a very, very collaborative approach to dealing with these issues. There is no financial institution that believes that it gets a competitive advantage from how well it does business continuity. Every institution understands when I learn something, I have to share that knowledge with everybody else in the sector because their health is just as important as my health when I'm dealing with business continuity. I need that institution to trade with. I need that institution to make payments to me. I need that institution to be able to continue to conduct my own business operations.

September 11th graphically demonstrated those issues. It graphically demonstrated that not having someone else in the system presented just as much of an issue to me as my own ability to operate. It demonstrated the interdependency issue that we have talked about. The loss of telecommunications was what the problem really was in those days and it also accelerated the shift away from this “one location” perspective. We understood that regional disasters can present serious business continuity issues even when firms located in a particular location is fine. My own company was fine on that day – we never had an issue on September 11th even though we were a few blocks from the Trade Center site. Our issue was what was happening to all of our members located in that region and the damage that had been done to their ability to continue to interoperate with us, so it was very much a regional issue and it brought that focus to the table for the first time.

The response to September 11th emphasized the importance of a lot of the issues listed on this slide. The core organizations, my own and others, said we have to begin dispersing our data processing capabilities. We have to begin developing DP capabilities outside of a particular region so that we do not have a dependency on a particular region. We've done that and many other financial firms have done that. We have to develop out-of-region business operations capabilities so that if something happens in a particular region, we can continue to operate by just shifting to another location and operating from that location. That also has been very successfully addressed by many financial firms.

We all implemented much more extensive work-from-home capabilities. People could interact and conduct their business lives from some place other than their offices. My own organization, for example, has a rule that members of the executive team can never be present in the same place at the same time. One member of the exec team always has to be offsite operating from home or somewhere else so that if something happens in the location where we are, that person is still around to be able to continue the operation of the organization. That effort has been very, very successful. These broad programs to upgrade business continuity capabilities have focused on the core and

significant layers that I referred to earlier – the core layer to ensure the payment systems can continue to operate, to ensure that the markets can recover very quickly and continue to operate, and to ensure that the significant participants in those markets can continue to operate regardless of what the circumstances are.

The events after 9/11 have, we believe – we know – validated the success of that strategy. The northeast blackout in 2003, the hurricanes in 2005 made very clear that the regional dispersion strategy was very, very successful. The lights were out in New York, but our business centers and our data centers located outside of New York were able to continue in operation without missing a beat. These events illustrated the success of the financial sectors collaborative response to this. We have a mechanism in place where people gather on conference calls very quickly when something happens and exchange information about state of health, ability to operate and so forth, and those mechanisms all worked perfectly in the northeast blackout very effectively at one in the morning, three in the morning and four in the morning, five in the morning. Having been on all those calls, they worked very well and people were able to interact very successfully at that time.

These events underscored the cross-sector dependency issues, obviously the issue at the time of Katrina. Financial services recovered very fast. Telecommunications took time and power took time, and we really were very focused on the need to address those issues as well. It also underscored that local issues are no longer local issues. One of the interesting learnings from the hurricanes – it wasn't so much Katrina, but Hurricanes Rita and Wilma were the ones that really underscored this issue – was that people in the sector needed to know what the response on the Texas coast and in Southern Florida were. What were the localities doing? Were they limiting movement? Were they shutting areas down? Were they evacuating people? Because we all have offices, we all have, conceivably, processing centers in those locations, and we need to know nationally what's being done in these local areas so that we have a full picture. It's no longer a local matter – we need to know what Florida is doing in terms of closing down facilities, for example, in response to a hurricane. That's something that now needs to be known nationally because most major financial institutions are now, at minimum, national institutions, if not global institutions.

So how does avian flu change this? Regionally dispersed facilities are great. They handle regional disasters very effectively. If the issue you are dealing with is something that is region-agnostic, however, and can occur in multiple regions at the same time, this no longer gives you the protection you think. Obviously we have no assurance that, in our case, our Tampa facility is going to be unaffected while our New York facility is affected or vice versa. Avian flu is something that can impact both facilities so this regional dispersion that we've very successfully done does not deal with this issue in and of itself.

Avian flu poses a longer duration challenge. Our business continuity strategies in banking and finance are very focused on surviving a reasonably limited period of time. In New York, we were knocked out of our office for the week of September 11th. On

Monday, September 17th we were back. We had to operate for four days under emergency conditions, but we were able to return to something approaching normality – aside from the smell – on Monday, September 17th. Business continuity strategies aim at dealing with relatively confined timeframes. Avian flu, as you well know, elongates that time frame quite a bit. You’re talking about a wave of infection that could be on the order of six to eight weeks, I believe is the estimate. You’re talking about multiple waves of infection being possible so that you might have a serious problem for two months, then come out of that problem, and then have another wave that could hit you several months thereafter and you have to basically go back into emergency mode. So business continuity plans have to evolve to address those challenges.

I will tell you that evolution is well underway, notwithstanding the New York Times this morning. This issue is drawing a lot of attention – certainly among the core financial components and the significant financial firms, in terms of the tiering that we talked through earlier. The collaborative capabilities that we have worked out over the last 10 years and tested in multiple situations over the last 10 years are operating very effectively to respond to this issue.

You all have in your packets this morning a document that the FSSCC issued two months ago, I believe, reflecting the first fruits of that collaborative sharing of information within financial services. That’s working very well. And the PCIS that Anne mentioned which is the cross-sector organization is also very effectively sharing information across sectors about what kinds of preparations are going on. There is an electric sector document on what they’re doing in relation to the potential for pandemic flu. There is a nuclear sector document: what they are doing in relation to pandemic flu. There’s materials the telecommunications sector has prepared: what they are doing in preparation for pandemic flu. The food and agriculture sector is developing a document on what they are doing. All of those documents are being made available and shared so that people understand what’s happening and also understand the implications for sector A of what sector B is doing, and we’ll talk about that in a minute.

Let’s talk briefly about a few of the details. For example, let’s take the issue of remote business operation centers. Today everybody operates collaboratively certainly in an emergency situation. Again, in a pandemic flu situation, if one were to develop, you can’t do that. You have to develop discrete organizational units that need to be functioning on their own and need to essentially be walled off from each other so that you are containing the possibility of people spreading a particular infection. The term of art that’s evolved to refer to this is “social distancing.” This involves developing teams that are essentially going to be operating in different locations and essentially not interacting with each other so that you’re minimizing the opportunity for an infection to spread among your employees. People are developing plans on how to do that.

Telecommuting is going to become a much more heavily utilized capability and some of the securities firms, for example, are figuring out how to have their traders trading from home. Do you move trading turrets into somebody’s house so that he can be trading from his living room so that he never has to interact with his counterparts? He’s

doing that all electronically. All of these “work-from-home” strategies are certainly something that every institution is trying to figure out how to build into its business recovery plan.

One of the decisions that we have in our business continuity plans – one thing that people commonly do – is to shut down what are viewed as non-essential areas. Reconciliation functions, for example, you suspend when something like this goes on because you say I’ll deal with those problems later – I’ll dig out a week from now, right? Reconciliation problems will always be there, so you say, “I’m going to take those people and use them for production operations and defer doing that function. I’ll deal with that a week from now or two weeks from now when the emergency is over.” Obviously, in the event of an avian flu pandemic, you can’t do that, because the time line you’re talking about is longer. Some of those operations that you thought you would suspend, you still have to resource. The clear example would be Human Resources staff people, who, under many business continuity plans, are automatically moved into production operations today. In a pandemic situation, you’re going to need them monitoring absenteeism rates; you’re going to need them monitoring health issues for your employees. So again you can’t suspend that function and your plan has to figure out how they are going to be able to continue to operate.

Every plan that I’m aware of is assuming that people will be grounded – that we are not going to have people traveling. We are not going to be allowing people to come visit our office; customer visits, for example, which obviously, under normal circumstances, would routinely happen. We suspend all that stuff. Our people are not going to be traveling. Certainly, as we get indications that particular regions of the globe are starting to see something that signals a potential outbreak of disease, you can expect that people will be suspending travels to such locations where there appears to be more potential of exposure to something. You will certainly see that as part of people’s plans.

Ongoing monitoring of absenteeism is something that you’re seeing built in to people’s plans. Circulation of absenteeism statistics to senior managers is something that people are working out how they’re going to do that – whether you’re going to have a dashboard that shows absenteeism rates as an example. That is something that people are thinking through.

And there is a whole set of issues that relate to interdependencies. The example, again, that everyone is using is the concern about telecommunications capacity and its impact on “work from home” strategies. The telecommunications networks are operating today in an environment where maybe 5 to 10 percent of people who work are roving workers and are relying on logging on to their home systems through the telecommunications network. If you now have a third of everyone working from home, what does that mean in terms of the telecommunications network’s ability to sustain that kind of sharp rise in volume? That’s an example of an interdependency issue that people are trying to think through. We have pretty clear advice from the telecommunications network folks that the core networks are going to be able to sustain that with no problem. The issue is the last mile in the community where your person is working from. How can

they log on to the core network through their local provider? Do they have what is needed to be able to do that? And if they do, that kind of volume surge, the telecom folks are telling us, would certainly be able to be sustained by the network, which is the answer obviously we're hoping to hear.

Another example is the local transportation issue. Every one of you knows that in the event there is a serious pandemic flu outbreak, people will think twice about getting on the metro trains to come in in the morning. So how are we going to deal with those kinds of transportation issues? Do we need to think through our ability to move people around? Do we need to change people's commuting patterns by having them operating from different locations? Do we want to have more people working from home so that we're not exposing them to that potential?

Firms will all take on a very big responsibility on staff communications. One part of pretty much every plan is providing much higher levels of education of the staff about hygiene and health best practices, getting down to how people wash their hands, or thinking twice about shaking people's hands when they come to meetings. Those kinds of things are topics firms will have to communicate to their staffs about because obviously preventing the infection from spreading is the best way of achieving the plan.

How do we communicate with local emergency organizations? How do we get information about local steps such as quarantines that are going to have a national impact? If the City of Houston decides to quarantine people or decides to declare what in the northeast we would refer to as a "snow day" – I don't know what they call it down in Houston – when only essential people are able to drive, nationally, we will need to know that. We need to know if a particular municipality is about to shut down my office by declaring a quarantine or by declaring a snow day. How that information is going to be circulated nationally is an issue that we've actually raised with DHS specifically because we think that's a role they're going to have to play.

Clearly, there is also a role on the regulatory side about communicating both domestically and internationally. We have to have the regulators operating consistently on the same issues. If capital relief, as an example, is given in one location, it has to be done consistently across other locations.

There are many health and safety issues that we have to focus on: principally, dealing with the issue of getting valid information. We all know the minute evidence of human-to-human transmission becomes clear, the hysteria that will become evident in the media is going to go straight through the roof. We need to be able to get access to sober and reliable information to be able to counsel our people about realistically how they should be thinking about these developments and realistically what measures they should be putting in place for themselves and their families.

And then obviously there are the X factors: what kind of stresses would a pandemic impose? What's the market reaction going to be when this information gets out? What kind of risk issues does that present? What kind of stresses on your risk

management operation does that create? Depending on how virulent the virus is, that may increase absenteeism rates, not so much because people are sick but because they don't want to come to work because they don't want to expose themselves. And again when you have the press saying the death rate is 50 percent, you're helping to get people very hysterical about this – clearly not a positive thing to do. And the issue I mentioned earlier on coordinated responses from local authorities will also be a problem for the sector as well.

I would say very clearly that among the core firms, among the significant firms, very, very serious planning efforts are well underway. I would be surprised to hear there are exceptions in that layer of the sector, although Ken, I know, believes there are some. The coordination is well underway. The industry organizations, FSSCC and others, are doing a lot of best practice sharing among themselves already. Financial sector guidance has already been distributed and I'm sure there will be more guidance in future – you have a copy of the FSSCC document in your materials. As I mentioned, cross-sector sharing of best practices is already in process. There is quite a bit of dialogue going on between FSSCC and the FBIIC members on this panel and we are going almost to the second generation of planning.

We've said we believe that we think one thing the government needs to do is to come out with a consistent and rational set of planning assumptions. We've all heard absenteeism assumptions that are all over the lot, you know. The only limit is 100 because you can't have more than 100 percent of your people out, but we're hearing numbers that are 20, we're hearing 30, we're hearing a third, we're hearing 40, we're hearing 50. We need something from the government that provides a consistent set of baseline assumptions that people can then plan from, because that will make our plans comparable across firms. And we need comparable plans because the next issue is going to be "I need to know what your plan is and I need to know are you doing things that are consistent with what I'm doing so that I can be reasonably confident that you're going to be there as a counterparty." And we are working through the possibility of a table-top exercise within the sector to start that process of sharing plans across institutions, which we would hope would happen in the coming months. So those are some of the examples.

That ends my presentation. Thank you very much.

(END OF SEGMENT.)