<meta name="viewport" content="width=device-width; initial-scale=1.0; "\>Event ID: 1904348
Event Started: 2/8/2012 8:00:00 PM
---

Please stand by for realtime captions.
>> Welcome and thank you for standing by. During the question and answer question you may put star and one if you want to ask a question. Today's conference is being recorded.
>> Welcome and good afternoon. Welcome to GSA FedRAMP media conference call. I'm going to make available after the call and audio transcript of the call today. I have everybody's e-mail address and I will send that out after this call. Here today we had David McClure the associated administrator for citizen services and innovative technologies with GSA, and his deputy Kathy and Katie and Matt. I will turn it over to her and three to make opening are marks and then we will proceed into the media briefing.
>> Afternoon everyone and thank you for joining us. We appreciate the opportunity to share an overviewof the FedRAMP ConOps document besiegers. We look forward to sharing how this will work and sharing your specific listings in the time that we have for that.
>> Let me introduceyou to FedRAMP and not will walk you through some of the specifics of ConOps it self . I think most of all online,I am sure you aware of what FedRAMP is and what it is trying to do . Thefundamental foundation of FedRAMP is trying to reduce the duplication and replication of work in the security area that is being used to monitor cloud of products and services. If we can get a uniform process in place, we can leverage of that authorization through the government instead of the replicating it agency by agency.
>> The fun-- the fundamentals of FedRAMP are consistent set of a flight controls, which we have reached everybody on prior to this. We use a third party assessment which has a -- and conducts briefings on how that will work. The use of the joint authorization board adds some weight to the review of the operations.
>> We hope agencies feel confident they can trust the assessment office and use it without replicating the same work. And FedRAMP, this was a continuous monitoring environment where we will not just rely upon annual testing of controls, operational, technical and managerial controls, but have some real time data on the operating environment of and provide real-time security awareness to agencies and to the federal government as a whole.
>> Or are many players who have been involved in putting this together. Both the standards, controls, the third-party assessment process and the way we want to operate the program. On the slide in front of you, you see some of the entities that play key rolesin the FedRAMP process. It is not just a GSA program , it has multiple participants and is designed to be a true governmentwide effort.
>> We coordinated the coronation -- the invention of the program with all of these entities with their feedback and clarification as we moved forward.
>> The real way of progression for FedRAMP is a phased approach and has days -- 4 basis. We are in the prelaunch phase where we are putting up guidance and educating the community on how this works. We are addressing concerns before we start. That is the period we are in now.
>> In June we plan to start up with what we call initial operating capability which will start-- jump start FedRAMP and will have a narrow intrigue into the program so we can kick the tires and make sure the process as we designed it is going to work smoothly and make adjustments as necessary on a real-time basis for this process and other things that we feel will make this operate efficiently as possible.
>> So we will go through a period of looking at a limited list of cloud services, starting out with the infrastructure of service area, and whatever pops to the top of the queue that we feel is the most benefit governmentwide.
>> Then we moved to full operations which is more of an open pipeline. We look at a diverse set of products and services, while still learning but not assuming that we have everything flowing fully into the JAB review process.
>> Been in fiscal your 14 , we will move into the sustaining operations and we will have more defined monitoring effort and we will operate in tandem with the controls that you saw published.
>> So it is a phased and calibrated implementation designed to learn, adjust and

correct as we go, rather than just jumpstarting and putting everything through this.

>> Agencies have a two-year window to be inconformance with FedRAMP . So we are not requiring everything through this process on the out that -- outset as well.
>> Lastly, there are a lot of things that we have been putting out and say putting as we get ready for thisstart up of the FedRAMP operations . Here are the list of things that we have been briefing and educating industry agencies, and to the press on today. This is the discussion onthe ConOps , and we still have some activity in the prelaunch phase to take care of, include in publishing the agency compliance guidance, actually a crediting the three PAOs, and analyzing the joint authorization board charter which is the group that actually does the provisionaloperations under FedRAMP .
>> So the roadmap to how we are proceeding, and trying to be as transparent and open as we possibly can be. I will turn this over to Matt who is going to give you a brief overviewof how the FedRAMP processable actually operate .
>> Yesterday we released FedRAMP  the concept of operation. I hope many of you have looked at that in advance of today's call. If not I want to do a brief overviewof CONOPS  to authorize them and continuously monitor them.
>> The three main process areas of FedRAMP are the security assessment, the leveraging  and the authorization. Then we move into what is called ongoing assessment and authorization, which most of you refer to as continuous monitoring.
>> The first step of security assessment has four distinct steps, initiating the request, documenting controls, performing security testing and finalizing security assessment. This aligns with 800-37. That first step of initiation, this is the only area of FedRAMP  that really has something new to it outside of what agencies do already.
>> Is as when -- providers work to commit their boundary and assets. I think that means control tailoring workload. Those are the only two newdocuments to FedRAMP. That is what cloud service  writers are coming in and Olivier be the responsibility of implementation to security controls.
>> So they will design -- defined as this is a cloud service, an agency responsibility or a hybrid responsibilities.
>> Along with that , there is a control tailoring workbook, were cloud providers look at all the controlsof the FedRAMP baseline , and determine if there are alternate limitations or other tailoring that they would do to meet that level of security those controls are intended to provide.
>> That is our first stage, is documenting those controls and the boundary and saying, this is how we are going to authorize the system going forward.
>> After you have done not, then the cloud provider uses this system security plan. This is basically the Bible of the security calls. -- Controls. It has all the FedRAMP baselines and they have to define the controller responsibility,  talk about what solution is being used to implement that control and how that solution meets the requirement of that control.
>> It is pretty fundamental, but it must be done for every single control and document within that system security plan.
>> The next step against that is, when you tested the system security plan. David mentioned talking about the word party assessor organization, this is where they enter this process. This is where you develop a test plan against that system security plan.
>> We use the 800-53Athat is tailored to meet all the FedRAMP  controls. That third party assessor will go against the test cases and will assess those control mutations and be sure they have met and draw liability tests and things like that.
>> Out of that, the third party assessor will generate a security assessment report. They will say that these controls are implemented fully, they may not be, the -- these are the risks the system poses to date.
>> Out of that you develop a plan of action, milestones or POAMs. This is a to do list that details all of the phone or abilities and controls that are not fully implemented, timelines and in her me -- intermediary actions to assess the older ability.
>> After that, then the cloud service provider has done all the work they need to do to create a completed assessment package. The cloud service provider will work to compile all that documentation and all of that will include a suppliers declaration of conformity and a -- station letter. This is the cloud service provider same

everything they are providing in the assessment package is true. They have implemented the controls like they said they have, third-party assessment results agree , and everything they are providing to us they attest as true and we can trust them on the period
>> After that, we submit the completed authorization package to the joint authorization board. They are going to review the package.Then the JAB will determine whether that is acceptable to the government and grant or deny a provisional authorization.
>> That completes the first process area which is the security assessment.
>> The second version is the leverage authorization. This area is something that had a lot ofthought put into it at the beginning of FedRAMP, because there were a lot of questions as to whether there could be one authorization that was made for the government. Could there be one entity or group of people who accept on behalf of the rest of the government ? That is not possible. Each agency must sign off and assess their risk for any data they place in an IT environment. So we created a provisional authorization and that is basicallya template authority to operate by the JAB . It is the same thing that an agency would issue themselves, you tell them the risk level of this cloud service environment, which you can leverage that authorization and use it at their own agency to make their own risk-based decision.
>> This is where this office comes in, the leveraging of that authority to leverage with the JAB .
>> Another thought process and things we have dealt withwith JAB and other stakeholders , is how to make sure that we really leveragethe power of FedRAMP . So the JAB only has limited resources to look at cloud service assessment recommendations at a time. So how can we have the most power behind the as we can.
>> They will have four different categories of assessment within the repository.
>> They will have a CSP supplied assessment package and that will be wherea CSP goes through and does all of the FedRAMP process , and submits a process to the PM, and they would be in queue to bereviewed by the JAB . The transit to look at the package and determine if it meets their capital level of risk.
>> The next two categories are agency authority to operate , one requires a 3PAO and one without. They are required to use FedRAMP when providing security authorization of any cloud service.
>> So after they complete that security authorization, they must submit that assessmentpackage to FedRAMP. So instead of holding until it has a JAB review, we are going to make this package is available for other agencies to leverage during that time, before a JAB review.
>> The final category is a jabber provisional ATOis a JAB has refuted and granted a provisional operation. They will also have a list of any subsequent leveraging authorizations by agencies.
>> So the third step is after that authorization has been granted, is moving into what most people refer to as continuous monitoring, but we call on going assessment authorization within FedRAMP. It involves a few more steps than what is involved in continuous monitoring.
>> This is in line with 800-137 and making a decision to move from a compliant based decision to a risk management framework. One of the main criticisms has been that the assessment and opposition process is really a picture in time from the day you authorize it until you reauthorize it the next time.
>> So we're trying to move from that authorization into that been an ongoing risk-based decision into the cloud environment.
>> Without there are three areas with ongoing assessment authorization that we are focusing on. One is operational visibility, two is change control and previous incident response.
>> Operation visibility, there is roughly 3 to 4 sets within us. We are talking about the automated data feed. And periodic reporting of controls. So cyber soap data feed and those real-time data feeds and implementation of certain security controls.
>> Also there are some controls that cannot be automated, and they will have periodic rigged -- reporting of those control implementations, either monthly, quarterly or yearly. They will be clearly defined.
>> And then the agency will review those automated data feeds and periodic reporting and determine if that system still maintains an acceptable level of risk for the government to place data in that system. It updates the authorization status

accordingly.
>> The second process is the change control process. This is when we're talking about the POAMs they talked about earlier, or the security to do list. And it offers changes to the cloud service and fireman.
>> This is where I do, PMO and security operation centers will be monitoring POAMs to make sure that all these actions are being addressed by cloud service writers in the time frame they said they would, and there is no new action item to present phone or abilities that is unacceptable to the government.
>> They will review any changes to the CSP system and a coordination with their change management plan.
>> This is when there are changes to the overall boundary, scope or services or hardware. And any significant changes that result out of the that may result in a reassessment of that cloud environment.
>> The final step in this ongoing assessment is it to -- incident response. This is where we coordinate with DHS and USCERT and the security operations centers. We are looking at incidences and a new vulnerabilities. We work with US CERT with agencies and the coordination looks into more holistic scale of mediation and what those agencies are.
>> Those incidents and new Boulder abilities would usually result in a POAM in the change process and any large enough might result in a provisional authorization decision determining whether that authorization should remain.
>> So that is a quick overview of the concept of operations. This final slide puts it all into one slide and is very complicated. But it is really the details of threedetails between the cloud service provider, FedRAMP and the government agency . It is the initiation, documenting controls, testing them and creating a finalized security package. This leads to the creation to an authority to operate and agencies leveraging not and I know the ongoing monitoring and assessment of activities around maintaining that authorizationwith FedRAMP .
>> With that I will turn it back over to Bob and we can open up for questions.
>> We will have the operator go over the how to ask a question process again.
>> Please press star one on your touch tone phone. To withdraw your question press star to -- two.
>> Our first question is from the call -- Nicole. They give a taking my question. With the operational capabilities of the services available in June , all the steps you mentioned and the process of going through the JAB operations, when you talk about a limited scopein his CONOPS, does that mean the number of providers and not a limited scope and services provided ?
>> I will answer that, this is Katie. We will answer all the steps that Matt just over. When we talk about limited scope, that pertains to two things. One is we can only process a limited number of applications at the beginning for several reasons. One of which is it is in the process and we have to see how it works and how long it will take. We will try to address any problems or deltas that occur so we can keep the process moving.
>> Secondly there are several things that are in the operational capabilities, most specifically more automated continuous monitoring, and a more robust repositoryfor FedRAMP argumentation that we are still looking at how to provide those services. Particularly with the repository, what security we need to implement so companies can comfortably while other security documentation and ensure it is only reviewed by valid customers and not by their competitors.
>> So there is anything I can put you to say this will not be available come Jan ? -- June ? I know you said a limited number of customers, but I want to make sure I am clear on what service will be available.
>> I think the process that Matt just went through will be available. I think there will be improvements in terms of the way the process will work. Secondly, we will probably have some lessons learned as we go through, so that'll be improved. That in terms of the basic process, our intention and where we are now is that will be available.
>> This is not, and to clarify, everything I talked about within your will be available for agencies andfor CSP atlaunchh. There is nothing you can put you that will not be available. What we are talking about a movie Teufel operations is the increase in certain capabilities. So the continuous monitoring at launch will be just what cyber scope does right now. We look at expanding the number of data feeds. Maybe moving from a paper-based -- repository to an electronic repository. All the

capabilities will be there , but it is increasing the capabilities within each one of those areas.
>> This is Bob and we are ready for the next question.
>> This is from David.
>> The controlsin the FedRAMP baseline  come from this 800-53R3 and I am sure you are aware R4 is due out later this month. Can you address will the baseline controls be updated to accommodate that ?
>> Yes. One of the benefits of that, and one thing we have talked about, is that they are issuing revision 4 very shortly and we have that -- we have not launched that you. So baseline will incorporate that. So assuming they released the revision before lunch,the JAB will update the security baseline  to include all the security updates.
>> Can you go into some of the controls that I've are responsible for the federal agency as opposed to the responsibility of the cloud service provider ?
>> If you look within the concept of operations, there is a diagram that eliminates the level of control. That is going to vary by CSP , as do it is the responsibility of one agenthe and the CSP . That is what at first initiation that we have to go through is important. The amount of control is duly needed and that, in terms of infrastructure, software and levels of response ability.
>> I saw the graph, but I'm hoping to get some sort of concrete example of this control is within the domain of the private sector as opposed to this domain as a part of the agency.
>> It is going to their if I -- very by the CSP  and I cannot point to one.
>> One thing that has to be clear, we are trying to make clear to CIOs end --, since there is not a one-size-fits-all model for these platforms, software, or infrastructure offerings, this is always an agency only and always a provider only responsibility. There are many variables that affect the bad outcome. What we are telling people or suggesting to CIOs and CITOs is 2 sure at least that is resolved. You don't leave that nebulous or assume that one party or the other is doing that.
>> Either through contract language or specification and the testing , that it is made clear how the agency and the CSP provider have that  Delaney a -- Delaney a good -- billing he aided -- decided.
>> Next question.
>> Based on what you said, it sounds like the answer may varyto my question by CSP, right now they are helping individual agencies connected there system. Will CHS [ Indiscernible - low volume ] and requiring that the status report to cyber scope and the second part of the question, how much oversight will DHS have ?
>> This is Matt. We are going to be following the same exact policies as DHS does now. So the current cyberspace policies to receiving those feeds will be the same as they are now. We are following the current guide in -- guidance.
>> So you're saying that private operations, even if it is an environment that is shared with nongovernment customers, they will have to share the data with GHS.
>> They will have to follow the GHS guidance.
>> And one quick question, when do you expect to have the list of the first batch of 3PAOs listed ?
>> Our goal is from the April.
>> Next question.
>> I tried to wait and not ask another question. [ laughter ] I am wondering with the templates that are mentioned, in terms of providing FedRAMP  cloud service level agreements, what type of range that would be an end when you expect to see that included ?
>> This is Katie and we are working on that now. The type of language, this would be more of a best practices. So we are currently looking at existing SOAs and contract language that would wedid for CSP  provision and also suggesting that practices to how this might be applied. When it comes out, it will definitely be released before an initial operating capability. And also, Matt has written a paper that is on this topic. You want to talk a little bit about that ?
>> It should be released through the CIO council and we are still working with the same groups that I worked with to create this paper. It is -- it is on best practices and the top 10 areas that the government needs to address within cloud computing. We are working with a group that made those recommendations to create contact -- contract clauses that agencies can leverage with their cloud contracts. But we will be releasingspecifically how agencies will comply with FedRAMP  , and

how they can places in the contract so they can make better requirements of their own agencies and address the uniquesecurity requirements within FedRAMP, such as data location and things like that .
>> Ready for the next question.
>> I guess there must not be too many people asking questions today. I wonder if I could go back to what I was asking about controls, because now I am confused. If the controls are dependent on the agency IT environment and the specific service that the CSP is offering, how do you achieve affordability of original authorization ?
>> The controller responsibility delineation is part of that security authorization or assessment package. So within that package, the control implementation summary worksheet, that determines whose responsibility it is to implement that control. So within agency leverages that assessment package, that the limitation of responsibility is the same across customers and for that CSP . That the limitation does not change according to that assessment package.
>> If the responsibility for the control various according from IT environment to IT environment, it is going to be rare that you get the same IT environment from one agency to the next.
>> What agencies are leveraging is the implementation of the controls that is the responsibility of that service provider. So that what -- that is what agencies are leveraging within that authorization.
>> Okay, thank you. Next question.
>> We currently have no questions.
>> Okay, we thank you forparticipating in the FedRAMP CONOPS conference call. Again I remind you to go toto the FedRAMP website shown , slide. We will post more ever -- shown on this slide. We will post more information and I will also post this transcript. We thank you for your participation, have a good day and we look forward to talking to use in -- to you soon.
>> [ Event Concluded ]