

<meta name="viewport" content="width=device-width; initial-scale=1.0; "\>Event ID: 2031304

Event Started: 10/25/2012 7:00:00 PM

-----

[ Please stand by for realtime captions ]

>>> Hello and welcome to our webinar. Four easy ways to get listed in FedRamp in repository. If you have a question for today, enter in the chat box, thank you.

>>> Hello. Thank you for taking the time to join us on our webinar, 4 ways to get listed in the FedRamp repository. I am the director of the federal commuting program, which is in the office of innovated technologies. FedRamp is a government wide program. Today's webinar will be led by Matthew, who is the project manager for FedRamp. Please use the chat dial log box if you have questions. Upload questions as they arise but we will not be answering questions till the end of the webinar. Again, thank you very much for your participation. We look forward to hearing your questions and I will turn it over now to Matt.

>> Thank you. FedRamp was developed to provide a standardized approach to security assessment, authorization and -- authorization and monitoring for cloud services. We will review thought repository is, benefits, how the repository is organized, the different ways to have authorization, and how they will use for security authorizations. We will be holding webinar on other topics in the coming weeks. The FedRamp repository is an online database of packages that meet the FedRamp requirements and mandatory by June 2014. This secure repository, how CS Ps can show compliance for customers. The packages include all the documents required to grant a authority to operate. Also known as a ATO which allows agencies to use the services. The repository is government reacted, owned and hosted through the executive office of the president, office of management and budget at a moderate security level. Each vendor received their own onclar in their repository. Access is controlled by the PMO and granted on an ad hoc basis to federal employees requesting access. The security authorize packages within the repository are uploaded by CSPs or federal agencies meeting the requirements for cloud services they consume. There are many benefits for being listed in the FedRamp repository. It is the site for the most current version of acuter authorization pack -- security authorization package. It has been tested by an independent third party. Agencies have confidence they can access security packages for review. The repository is also a one stop shop for federal agencies and CSPs. For CSPs you have one site to maintain the current version of your security documentation. Agencies have one site to view security authorization packages. Being listed in the repository can be a business discriminator for CS Ps. Federal agencies are required to consult the FedRamp repository when conducting security authorizations. TheyThey will also

use it to understand the landscape. A CSP is demonstrating their ability to meet requirements, cut down the time for deployment of a cloud service by federal agencies.

>> I am sorry to interrupt. This is Katy. Questions are already coming in. But please restrict the topic of your questions to the topic of the webinars so we won't be talking about FedRamp in general. If you have questions on other topics we will have additional webinars in the coming weeks. Right now we would like to restrict the questions about questions about the repository itself.

>> Thank you. The repository is organized by the level of government review. FedRamp repository organizes security authorization packages based on the level of government review and who provided the authorization for leverages. At the highest level of review is a job provisional authorization. Granted by the joint authorization board. They will reflect ATO granted as well as any agency whose leveled that authorization. The second highest level of government review is a security authorization package that use the FedRamp accredited APO. A agency ensures that CSPs meet the requirements and the CSP was assessed. Next are the security authorization packages with a agency ATO. Federal agencies have ensured CSPs meet the requirements but did not use an accredited -- for the independent assessment. All packages will not be eligible in this category for review by the job for authorization as they do not meet the requirements for assessment. Finally there is the CSP supplied security authorization packages. Packages have not received an ATO from an agency or from the job. This is a package by the CSP using an accredited -- to provide independent assessment and reviewed by the PMO for completeness. No risk assessment has been conducted. They established these categories of security authorization packages to accelerate leverages. There is no need for agencies or CSP to pate for authorization to begin work. They allow agencies to begin to mead FedRamp requirements for the June 2014 deadline now and CSPs can work independently, with an agency or with FedRamp to be listed. There are only 3 requirements for being listed within the FedRamp repository. These requirements aligns with existing federal information security policy frame work and guidelines. As required through the federal information security management act and the 800 series documents through the national institute. Three requirements must be met before being listed in the repository. First, CS Ps must implement and address security controls. FedRamp has baselines, they are a selection of controls from the special publication security control baseline with additional controls selected to address the requirements of cloud computing. A full listing can be found on FedRamp.avi. FedRamp-- FedRamp.gov. This assessment must have been completed by independent 30 party organization. Proof is satisfied through a assessment report created by the independent assessor. Third and final, CSP must complete all the requirementd documentation, templates - - required documentation. Templates help provide consistency in review by FedRamp and agencies. Requirement three is all documents are completed and included within the security package. All of the documents required are listed in section 10 of the FedRamp concept of operations. All of these documents have templates on FedRamp.gov. They are divided into two types, mandatory and non-mandatory. The mandatory are the three key documents for any security authorization package, the system security plan, security assessment plan and security assessment report. The system security plan is the cornerstone document for the security authorization package. This document describes the system and identifies how all the security

controls are implemented for that system. The security assessment plan describes the assessment they use against the test cases. The security assessment report contains the independent assessors results from testing, all collected evidence from the testing and a report on the implementation of the controls that koodescribe all vulnerables and security weaknesses -- that describe all vulnerabilities and security weaknesses. If templates are not used CSP must -- examples of the documents include, the control work book. This identifies the security controls that have been adapted by the cloud source provider for implementations that are different. The management plan, this identifies how the cloud provider makes changes in the operating environment and the plan of action and milestone, this document's planned action by the provider to change or implement security controls to address weaknesses within a CSP system. Once a CSP met the requirements for being listed in the repository, there are four steps to submit your documentation to be listed. First, you must apply at FedRamp.gov. After review they will schedule a call with the CSP and create an onclave within the repository. Next they will grant access to the CSP or agency. Then the CSP or agency will upload the documentation. And the third step, the PMO will check for package completion, this will ensure all documentation is included, all security controls addressed and all documentation is completed. During this phase the documentation will only be available by the requesting organization and the FedRamp PMO. Once the security authorization package is complete, FedRamp.gov will be updated to reflect the package as being available by leverages. At this time agencies can begin to request access to review the security authorization package for use of their agency in granting a ATO. Now you are listed on FedRamp.gov and have a security authorization package available for leverages. How will they do this? First, when deploying a product or service, a federal agency must search the repository for documentation to leverage. The information provided on FedRamp.gov about the repository will list information only about the CSP, the service authorized and when it was authorized, what level of authorization was granted and any ATO. If an agency searches the repository and finds the CSP has a package listed in the repository, the agency must request access to the security authorize action package from the PMO. They must then review the package and use this as the basis for granting ATO. As part of their review agencies must examine security -- and are responsibility for implementing all customer responsibilities controls before granting an ATO. Finally, CSP must implement a continuing monitoring program. The CSP must provide artificates in support of the program -- artifacts in support of the program. During this webinar we reviewed the four ways a CSP can be listed in the FedRamp repository. First, CSP must meet all FedRamp requirements, using the security controlled baseline, using a independent assessor and completing all of the required documentation. Then we reviewed the different categories of security packages available in the repository, CSP and agencies can begin work now and don't need to wait to meet federal requirements and be listed within the repository. Next we detailed the FedRamp templates describing the temptlets available. Then we discussed how CSP and agencies submit authorization packages for inclusion within the repository and detailed how agencies will use the repository in granting ATO for CSP services. And last, the first step in being listed in the repository is to apply on FedRamp.gov. We would now like to open up the session for questions. To ask a question, use the chat dying log box within the go-to meeting. We will do our best to answer all questions but if we don'tp get to your -- don't get to your question we will answer it on FedRamp.gov. At the conclusion we will go over the list of upcoming webinar. You

canning also commit questions to [info@fedRamp.gov](mailto:info@fedRamp.gov). Your questions will be anonymous so please ask away.

>> First question is, who do we e-mail to get access to the onclave? FedRamp.gov and will be contacted by the PMO. Second question, will the repository maintain current weaknesses identified through various means such as audits and continuous monitoring with a ring assessment for individuals to review when needed? Yes. Cloud service providers will provide information to the repository throughout the life cycle of the security authorization process and through their continuous monitoring program.

>> Third question, will an agency be able to see a CSP's package? Yes. They will be granted permission to see the entire package.

>> Can you please describe what is in place to ensure CSP documentation is not shared inappropriately. Federal agencies are granted controlled access. Federal employees are governed by the trade secret act and they sign non-disclosure agreements.

>> How many CSP are listed in the repository? There are currently no CSP listed in the repository.

>> We are processing the large number of questions that are coming in so there might be a few pauses while we make sure we are not repeating questions so I apologize for silence you experience for a little bit.

>> Can a CSP choose their own independent third party assessor? Yes. The relationship between -- it is chosen by the CSP and paid for by the CSP.

>> Are more 3PAO being added? Yes, it is on rolling admissions and we are still accepting applications and processing them as they come in.

>> Can the general public access the listing of authorized CS Ps? The list available for viewing will be available publicly. All security authorization documentation will only be available for viewing by federal agencies. Authorized for viewing by the PMO.

>> Is there a way to tell what CSP applied? No. We will not be releasing that information. But we are -- we have received over 60 applications and are processing all of the applications and reached out to every vendor that has applied.

>> You mentioned common requirements, do you anticipate inclusion for any other requirements? FedRamp is based off of requirements, while we take into account other security recommendations and programs, we are based windages and do not plan on -- based -- and do not plan on including any others in our requirements.

>> Where can we find a 3PAO and do we recommend any? All three that have been accredited by FedRamp are available for viewing on FedRamp.gov. FedRamp does not promote any 3PAO over another. We believe all can provide the same quality of work.

>> What prevents one CSP from viewing the package of another CSP? Each vendor is given their own onclaim within the repository, they can't see any other onclaves within the repository. There is security and access control mechanisms. We are more than happy to provide review of the security documentation before you place any of your documentation in there.

>> Will government providers have access to ensure we are using approved cloud providers? Yes. Government customers, providers can see the public listing of who is in the repository and if they would like to see the security documentation can get that granted through the FedRamp PMO.

>> Can you clarify the benefits of being in the repository but not having the FedRamp review? We designed the FedRamp repository to insurge leverages by agencies. We believe -- encourage leveraging by agencies. The joint authorization board said they did not want to limit the repository to those cloud providers that already had government contracts which is why we are allowing CSP to provide packages and due to the limited resources they did not want to limits only packages within the repository to be those authorized by them. The benefits are that federal agency can see -- agencies can have one place to see where they have authorized cloud services and promotes leverages at a faster pace than currently available throughout the government.

>> When do you expect the first approves CSPs to be listed on the FedRamp website? We expect the first list of CSPs granted a provisional authorization through the job by the end of the calendar year. However, packages available through agency ATO and provided by CS Ps will become available as soon as they are submitted to the FedRamp PMO.

>> What was the June 24 deadline you mentioned? All FedRamp launched on June 6, 2012, part of the nature was that any future cloud services that were purchased after June 6, 2012, had to meet FedRamp requirements. For currently implemented cloud services they had two years to update to the FedRamp requirements, June 6, 2014.

>> Can a CSP contact 3PAO directly? Or is there a formal process for initiating a assessment? CSPs can directly contact them and work with them independent of the FedRamp office. If a CSP is working with the FedRamp PMO for a job authorization, the FedRamp ISSO will work with the CSP and 3PAO once they are selected to make sure all expectations are met.

>> When will the repository be available to agencies? It is available now to agencies. And will be populated with security authorization packages as the FedRamp PMO receives them.

>> It is also available for cloud service providers if they have security authorization documents they would like it provide to the PMO and make listed as well.

>> Is there a difference in requirements for providers a vendor hosted cloud versus private? No there is not a difference in requirements for public or private.

>> Do agencies need to utilize independent 3PAO to say assess their package? Agencies are required to utilize independent assessors to assess their package. Agencies are not required to use a FedRamp accredited 3PAO but are encouraged to do so because we have accredited

them according to Independence and their knowledge. It will allow the CSP to have a job review for a potential provisional authorization by the job.

>> If the security assessment package category, does that prevent or allow a agency to use that CSP? If allowed does the CSP still have to go through an assessment? Agencies can accept the CSP provided package granted they do a risk assessment. All packages in this category will not have a risk review done by the FedRamp PMO. There will be a completion review to make sure all requirements have been met but a agency will have to be the first person to do the risk review of that system from the SSP all the way through.

>> We received a lot of comments asking if the slides and questions will be available after the viewing, we will make the slides and the question and answer session available on FedRamp.gov after -- by next week.

>> How many agencies are there in total that will be leverages the repository? Potentially every single federal government agency.

>> After this call where can one get questions answered? On the screen you can see our website as well as our e-mail information at FedRamp.gov.

>> For a project that has an agency ATO that was not performed by a accredited APO -- agency ATOs can be leveraged by other agencies, that is why we are including them within the repository. If a accredited 3PAO will not review because it doesn't meet the Independence requirements by using an Independence accredited 3PAO. Yes, an agency ATO, as long as it meets the FedRamp requirements and listed in the repository, can be leveraged.

>> The June 2014 deadline is still presenting confusion. The repository is available now. The June 2014 deadline is when all cloud services that agency use must meet FedRamp requirements, however, the repository is available now for federal agencies and CSPs and will be populated with security authorization packages as they become available.

>> There is also confusion about whether the poams were mandatory. The template is not mandatory however they are a mandatory document that needs to be a part of any security authorization documented and will need to be updated on a regular basis.

>> What is the anticipated time frame between applying and being inaged with the FedRamp -- engaged with the FedRamp PMO. The FedRamp PMO contacts within one week to understand where -- which process the agency or cloud service provider is seeking within FedRamp, a joint authorization board, authorization or wishing to have a completed documentation listed in the FedRamp repository. The process includes an interview, in which we assess the readiness and requirements to be listed in the FedRamp repository. To date every single applicant has been contacted by the FedRamp PMO.

>> Can we add documents to the onclave as they are completed? The FedRamp PMO can work with providers to make it work for them in the best way possible. We don't have a defined process that does not allow that to happen. We can work with each vendor to see what works for them.

>> What is the difference between a job authorization and having a agency authorization in the repository? The job authorization provides a heightened level of government review. The joint authorization board is comprised of the -- for a job authorization these three CIOs reviewed the security authorization package provided by a cloud service providing and recommending they can accept the risk so that agencies can use that CSP. An agency ATO or authorization means only a singular or multiple agencies reviewed that provider's security authorization package and they provided a risk review, not the joint authorization board.

>> Will you post the Q&A from today? It will be a part of what is available on FedRamp.gov next week.

>> Can you state the four ways to get approval for FedRamp to be listed in the repository one more time.

>> First, there is the job provisional authorization. Second, an agency ATO that utilize a FedRamp accredited 3PAO for the assessment. Third, an agency ATO that did not use a accredited APO and a cloud service provider supplied authorization package without an ATO.

>> Is an onclave established once per incidence or per service? Established for a cloud service provider and further downed by preserve that cloud service provider -- by that cloud service provider.

>> That you can thank you for all the -- thank you for all the questions. To conclude, we will be holding webinar over the coming weeks to address other questions. -- weeks to address other questions. November 7, we will discuss how CSPs and agencies can get started with the FedRamp security authorization process. Future webinars will address documenting the FedRamp security controls. Assessments and completing your security authorization package. And security authorization packages across infrastructure, platform and software. As always for more information please contact us or visit us at any of the following websites. FedRamp.gov or through e-mail. [ Event concluded ]