Industry and government observers are optimistic that plans to streamline and enhance a government program designed to boost adoption of secure cloud computing will encourage more agencies to commit to the program.

Launched about 2½ years ago, the Federal Risk and Authorization Management Program (FedRAMP) provides a centralized, standard way for agencies to procure secure cloud products and services.

FedRAMP may be simple in concept, however, it has proven more difficult to implement than anticipated, in part because the process is confusing for agencies, according to industry and government speakers at a Face-to-Face event on January 22 titled, “FedRAMP: The Path to Success.”

“So far, FedRAMP has saved the government $40 million in cost avoidance, and approved 29 FedRAMP-compliant cloud vendors and more than 30 accredited Third Party Assessment Organizations. However, FedRAMP officials had

“We want to make the program more effective, make the program move faster, make sure everyone understands it. That’s what these [two-year] priorities are designed to do.”

Matt Goodrich, FedRAMP, Director
GSA Office of Citizen Services and Innovative Technologies
hoped more agencies would be using the program by now.

**Charting a future course**
The General Services Administration (GSA), which runs FedRAMP, recently released a two-year roadmap designed to clear up some confusion and garner more support for the program. “We want to make the program more effective, make the program move faster, [and] make sure everyone understands it,” said Matt Goodrich, FedRAMP Director at GSA at the event.

Highlighted in the roadmap are plans to increase stakeholder engagement through such things as working groups; improve efficiency by enhancing automation capabilities, among other things; and continue to adapt, by publishing a continuous monitoring roadmap, for example.

GSA is also hoping that agencies turn to their peers for help, building on the work that has already been done by early FedRAMP adopters, such as NASA and the Department of Health and Human Services (HHS).

“We have a process and I’m willing to share it,” said Chris Bollerer, Director, Security Governance, Risk Management and Compliance at HHS. “We need the entire federal community to step up to the plate.”

Cloud service providers are another good resource for help in implementing FedRAMP, but agencies must do their own due diligence, too. “FedRAMP won’t save you from a poorly written or poorly executed application,” said Chris Spina, vCloud Government Service Specialist, VMware.

**Not a one-size-fits-all**
While there is no magic formula for FedRAMP, nor is there a one-size-fits-all approach to get to the cloud, there are steps that agencies can take to make the process work for them, according to speakers at the event.

From the beginning, agencies should garner broad support and buy-in within their organization, manage expectations, bake security into every requirement, clearly articulate expectations with cloud service providers, take a phased approach, and know what they want to get out of the program from the start.

“You have to know what outcome your customers or stakeholders are going to need,” said Roopangi Kadakia, Web Services Executive, Office of the CIO, NASA.

Also, agencies must manage their risk when moving to the cloud, which doesn’t mean “fixing every vulnerability,” said Kelley Dempsey, Senior Information Security Specialist, NIST IT Laboratory/Computer Security Division. “But it also doesn’t mean doing nothing.”

Vendors like the program because it “makes transparent” the process they must follow to provide services to agencies, and agencies benefit from having “a repository that is a definitive authoritative” place to procure cloud services and products, said Mike Younkers, Senior Director, Systems Engineering, U.S. Federal, Cisco Systems.

FedRAMP has “recalibrated” the Federal Information Security Management Act, which had become more of a paper drill, said Nick Son, Managing Director, Technology Advisory and Assessment Services, Coalfire Public Sector. Embrace it, he said, “don’t fight it.”

At the end of the day, agencies and vendors agree cloud computing makes good business sense by offering increased scalability and cost savings, and FedRAMP provides a secure way to get there.
TOMORROW starts here.

Today, it’s easy to marvel at how far we’ve come.

Our phones talk to our TVs to record our favorite shows. Doctors in Estonia diagnose patients in Denmark. Social networks help companies improve customer service.

And yet, up to now, more than 99% of our world is not connected to the Internet.

But we’re working on it.

And tomorrow, we’ll wake up pretty much everything else you can imagine.

Trees will talk to networks will talk to scientists about climate change.

Stoplights will talk to cars will talk to road sensors about increasing traffic efficiency.

Ambulances will talk to patient records will talk to doctors about saving lives.

It’s a phenomenon we call the Internet of Everything—an unprecedented opportunity for today’s businesses.

Tomorrow?

We’re going to wake the world up. And watch, with eyes wide, as it gets to work.

#tomorrowstartshere
Session Highlights
Here are some take-aways from the individual sessions

SESSION 1
FedRAMP: The Two-Year Roadmap

Speaker: Matt Goodrich, FedRAMP, Director, GSA Office of Citizen Services and Innovative Technologies

GSA’s two-year roadmap for FedRAMP is designed to make the program easier and more efficient for agencies by:

- Increasing stakeholder engagement: establish baseline metrics, boost the number of agencies implementing FedRAMP, create multi-agency working groups, launch FedRAMP.gov and online training.
- Improving efficiency: update 3PAO requirements to enhance quality of deliverables, identify automation capabilities and requirements for automated tools, draft requirements for re-using industry standards.
- Continuing to adapt: publish continuous monitoring roadmap, establish high baseline for public comment and identify other agency baselines, draft initial FedRAMP overlay to other IT policies to avoid duplicate efforts.

SESSION 2
FedRAMP Essentials: Implementation Strategies Mapping the Road to Authorization

Speaker: Chris Bollerer, Director, Security Governance, Risk Management and Compliance, Department of Health and Human Services

HHS was the first agency to sponsor a cloud services provider. Here are some lessons learned:

- Clearly articulate expectations with CSPs and ensure they understand the process.
- Involve stakeholders at all levels throughout the process.
- Collaborate with FedRAMP PMO.
- Identify deal breakers, unacceptable risks early on.
- Clearly define repeatable processes that meet agency requirements.

SESSION 3
FedRAMP Essentials: Best Practices and Lessons Learned

Speaker: Roopangi Kadakia, Web Services Executive, Office of the CIO, NASA

- NASA has migrated 158 web applications into the production cloud environment managed by the WESTPrime contract.
- What makes a good candidate for the cloud? Expiring contract; end of lifecycle; requires up and down scaling to support variable processing requirements; is a FISMA low/moderate website or application; needs better security, privacy.

SESSION 4
FedRAMP Essentials: Putting Guidance and Standards to Work

Speaker: Kelley Dempsey, Senior Information Security Specialist, IT Laboratory/Computer Security Division, NIST

- One size does not fit all when it comes to the cloud.
- Cloud providers have to comply with FISMA and protect information at the appropriate level.
- Can’t eliminate risk; just manage it.
- The cloud risk management framework under development adds cloud specific tasks to the normal risk management framework. Initial draft expected by end of summer.
- FedRAMP baselines build on SP 800-53. High baseline for FedRAMP is out for review.
Session Highlights
Here are some take-aways from the individual sessions

**SESSION 5**
FedRAMP Tools and Tactics

**Speaker:**
Chris Spina, vCloud Government Service Specialist, VMware

- It takes a high level of investment to get through FedRAMP process and come out with an ATO.
- Agencies should look at the definitive repository of where a vendor is in the FedRAMP process so they know what they’re really getting.
- Early adopters are great resource for information about getting started with FedRAMP.
- One size doesn’t fit all on cloud.

**Speaker:**
Nick Son, Managing Director, Technology Advisory and Assessment Services, Coalfire Public Sector

- FedRAMP is not a thing; it’s a process.
- Cloud is modular.
- An agency’s security budget has to be thought through carefully and must be clearly defined for all procurements.
- CSPs should know their assets, think about whether to incorporate corporate network into their search provider boundary, and should document everything.
- Cybersecurity professionals should be at the table and have a say in the cloud decisions.

**Speaker:**
Mike Younkers, Senior Director, Systems Engineering, U.S. Federal, Cisco Systems

- FedRAMP makes transparent the process for vendors to provide services to agencies.
- How should agencies get started with FedRAMP? Start with FedRAMP PMO office, CSP, and other agencies such as HHS.
- Cisco envisions an inter-cloud like the Internet, which makes it difficult to work through boundaries when trying to partner with other CSPs.
- Open source is a philosophical conversation and something agencies need to flesh out with their CSP.

“Cloud providers have to comply with FISMA and protect information at the appropriate level.”

KELLEY DEMPSEY,
SENIOR INFORMATION SECURITY SPECIALIST,
IT LABORATORY/COMPUTER SECURITY DIVISION, NIST
Our combination of Federal Agency and Cloud Server Provider experience helps streamline the security assessment and authorization process.

Learn more at:
www.CoalfirePublicSector.com
CDM-FedRAMP union not on the calendar... yet

BY MARK ROCKWELL
OCT 21, 2014

The General Services Administration is looking forward to providing continuous diagnostics and mitigation services through the federal cloud authorization program, but that effort faces some challenges before it becomes a reality, according to a top CDM manager at GSA.

“At some point, the two will marry,” said Jim Piche, manager of the agency’s Federal Systems Integration and Management Center DHS Group. Although GSA is a strong proponent of cloud-based services, implementing CDM through the Federal Risk Authorization and Management Program needs a little more time, Piche told an Oct. 21, 2014 ImmixGroup panel on detecting insider cyber intrusions.

While GSA is working to bring FedRAMP cloud capabilities to bear on CDM services, CDM’s structure—which includes a phased model that considers groups of large, medium and smaller agencies, blanket purchase agreements and more than a dozen providers—complicates coupling it to FedRAMP. Additionally, Piche said, FedRAMP is building to a medium-level security baseline, while CDM, given its specific security responsibilities, requires a higher level baseline.

GSA is working to move past those challenges, he said, but no timeline has been set.

Meanwhile, GSA and other agencies have been learning the ropes as agencies implement Phase 1 of CDM’s three-phase roll out.

The first phase, which looks at endpoint device security, has given federal IT managers who have implemented it a sprawling view of the devices and vulnerabilities on their networks, many of which had gone unnoticed under previous monitoring regimes.

When CDM was implemented at the Securities and Exchange Commission, “we were shocked” at the number of vulnerabilities it revealed, said SEC CIO Tom Bayer. His agency has been busy implementing its own version of CDM, but signed a memorandum of agreement with GSA at the beginning of September to use GSA’s CDM contracting vehicles.

“We’ve seen benefits,” said Tom DeBiase, chief information security officer at DHS’s Immigration and Customs Enforcement. When his agency began implementing phase one and taking inventory of endpoint devices to secure, “we had a lot more technology than we realized.”

Although GSA and DHS awarded the first CDM task orders in January, Piche said a second series of contracts, under Task Order II, are in varying stages of completion—from evaluating submitted vendor proposals for larger agencies to releasing and drawing up vendor solicitations for smaller agencies. Task Order II focuses on products and services surrounding planning, management, training, architecture and engineering.

Federal CDM dashboard solutions are currently under evaluation by DHS, according to Piche. “There has been no competition, no selection and no award” for the dashboard contract, he said.

DISA releases draft of new cloud security requirements

BY SEAN LYNGAAS
DEC 12, 2014

The Defense Information Systems Agency has released a draft of a security requirements guide for cloud computing across the Defense Department. When finalized, the SRG would supersede and rescind current guidance under the Cloud Security Model. When that guidance is published, cloud providers being assessed against the CSM requirements must comply with the new SRG “in coordination” with their next annual FedRAMP reauthorization, the draft states.

DISA, the agency in charge of the IT infrastructure underpinning DOD missions, has been updating its security guidelines to clarify for commercial cloud providers what it will take to operate sensitive and classified DOD information.
As acting director of the General Services Administration’s Federal Risk and Authorization Management Program, Matthew Goodrich is tasked with both enabling and encouraging agencies to embrace the standardized governmentwide framework for cloud security.

FCW’s Mark Rockwell spoke with Goodrich about the progress to date and the outlook for 2015. Below are excerpts of that conversation, edited for clarity.

What is the outlook for FedRaMP in 2015? What are the priorities?

In the next six months, you’ll see a two-year road map that will highlight our priorities over the next six, 12, 18 and 24 months. One of our key focus items is going to be making sure that we engage with agencies much more directly and help them complete and achieve more FedRAMP [authorities to operate] and make sure they’re FedRAMP-compliant.

You’ll also see us publish a lot more guidance, education and training modules for our stakeholders—first in a more generic, open-to-everybody manner and then more directed at specific stakeholder groups as we continue to expand the knowledge base and training.

You’ll also see us focus on the efficiencies of the program, incorporating lessons learned back into our documentation. Also, we’re looking at how effectively we’re using our [third-party assessment organizations’] work product to cut down some of our review cycles based on the quality of the products they’ve delivered to us, as well as aligning cloud providers with the most appropriate path for them to get authorization, whether that’s the Joint Authorization Board, through the agency or directly through the [cloud service providers].

We will continue to grow, mature and adapt the program. We’ll continue to work with the [Continuous Diagnostics and Mitigation] program at [the Department of Homeland Security], so that we’re aligned as we move forward. We’ll also work with the [Trusted Internet Connections] program, as well as finally beginning to address the high [security] baseline that our stakeholders have been asking for, for a while.

How many agencies have achieved FedRAMP compliance? What is your advice for agencies trying to attain compliance?

Our insight into compliance is through PortfolioStat reporting and analyzing that data, as well as looking at some other data points provided by service providers that we’re working with or through other data, like [Federal Information Security Management Act] reporting. So we have a pretty good grasp of what agencies are doing.

I think, though, that we are going to be directly engaging with agencies more to help them bring either those existing authorizations up to FedRAMP compliance or understanding if they’ve already come up and they haven’t shared them with the [program management office]. I think there’s probably some of that happening, too.

We have to really make sure we’re engaging with our agency stakeholders to help them more efficiently upgrade their existing authorizations or get them to work with their current cloud providers to work through an authorization. We have to make sure they understand the value of FedRAMP across the federal government and what it enables.

What has been FedRAMP’s greatest strength? What’s most encouraging?

I started on the federal cloud computing initiative five years ago, and everyone at that point said the cloud wasn’t secure. I think it can’t be underscored enough that FedRAMP actually shows that cloud is something the federal government can use securely.

In a little over two short years being in operational programs, we’ve been able to show that 160 business systems reside in FedRAMP-authorized systems, as well as demonstrate roughly $40 million in savings [compared to the cost] if each one of those had been authorized individually.

Just underscoring the value of the fact that the cloud is secure and can be used—coupled with reuse and overall cost savings in just the short amount of time we’ve been up—I think is one of the biggest strengths we can show.

There has been criticism of the FedRAMP process as burdensome and prone to bottlenecks. How would you respond to those criticisms?

That’s why we’re trying to engage with our agencies more directly so they understand the process and the intent behind it. FedRAMP didn’t intend to change the processes by which agencies authorize IT systems. We wanted to
The Fastest Path to Cloud for Federal Organizations

Overcome your lingering obstacles to cloud adoption with VMware vCloud® Government Service provided by Carpathia™, an enterprise-class hybrid cloud service built on the same platform used in so many federal data centers today.

- Test and Development
- Packaged Application Hosting
- Backup & Disaster Recovery
- Web Hosting & Customer Service
- On-Demand Data Center Expansion

Learn more at
Carpathia.com/Learn/VMware-vCloud
ensure that agencies did it consistently between one agency to another so the federal government had a standardized way to assess risk in a cloud environment [and] so agencies could reuse it.

In making sure agencies fully understand what it means to be FedRAMP-compliant, I still think there is some confusion out there about what it takes to do that and the varying levels of review.

**Is there a little bit of fear, too—a fear of the unknown?**
Culture change is not unique to the IT landscape. There’s always going to be an amount of culture change, and anytime you outsource something to another entity, there’s going to be some hesitance.

However, we’ve been able to show that government agencies can do it and have sustained levels of security.

**How do you explain FedRAMP’s complexities to federal agencies?**
That is the challenge. FISMA is complex, and what we’re focusing on is making sure it’s clear and straightforward. If you try to simplify FISMA and FedRAMP, you miss some of the nuances.

What we’re trying to do with our guidance is make sure that complexity is communicated in a very clear, straightforward way so that it’s easy to follow but not that it is something that is overly burdensome or too hard for agencies to do.

We’re looking to engage with agencies that think it’s daunting or really complicated, and walk them through the process and make sure they understand exactly what it is.

**Is there anything people will be surprised to see in the new two-year road map?**
I don’t want to say no because that makes it sound like everyone knows what we’re doing. I think it’s what you would expect with any program that’s at our maturity level.

We’re roughly two-and-a-half years in. We reached our mandatory compliance date in June, so we’re trying to make sure that that compliance number goes up and reaches the highest it possibly can. We’re going to focus on some key initiatives around that.

You had mentioned there are some criticisms of FedRAMP being overly burdensome or taking too long, so we want to make sure it’s truly as efficient as possible, without lessening the rigor of the security assessments. We will continue to grow it out. We don’t want to be a stagnant program.

Those are some of the key goals. I don’t think any of that would be shocking. Those initiatives will make it much more clear.

**What is the current compliance rate?**
Through the PortfolioStat data that we have, we would estimate that agencies are anywhere from 25 percent to 40 percent compliant.

**What else can you tell our readers about what they should be doing or what they should expect from FedRAMP?**
We launched FedRAMP Ready [in October]. That’s part of the PMO’s goal of helping CSPs who are ready to begin an assessment and authorization with federal agencies. We’re highlighting those CSPs on our website that have demonstrated the initiative to meet the federal requirements.

The providers that are listed there have gone through a readiness assessment by the GSA program management office. They have a baseline of documentation and are ready to begin with an agency [on] assessment and authorization. That’s something we’re excited about – getting cloud providers through authorization faster.

Also, agencies are procuring more and more cloud services, so we’re working to get out more specific guidance on how agencies should put FedRAMP into their contracts and what they should require from their cloud service providers.

**How specific is the guidance?**
Right now on the website, we have template contract clauses and template language. We’re looking to expand that language for agencies when they’re considering putting a contract out for cloud services.

We’re seeing some procurements come out that show agencies requiring a FedRAMP authorization at time of award. With the number of CSPs that are authorized at the FedRAMP level now, it’s hard to have a competitive marketplace for some services. It’s a little unduly restrictive and premature to have those, so we’re making sure we put guidance into the requirements so the contracting officers know exactly what it is agencies should be doing in terms of requiring FedRAMP authorizations, as well as when they can.

**Is FedRAMP living up to its potential?**
I think where we are at two-and-a-half years, absolutely. There’s always room for growth, and we’re excited to continue on the path that we’ve made.

NIST marks top security requirements for government cloud

Cloud computing offers both unique advantages and challenges to government users. The advantages are well-advertised: Greater efficiency, economy and flexibility that can help agencies meet rapidly changing computing needs quickly and cheaply while being environmentally friendly. Among the challenges, security is the most commonly-sited concern in moving mission-critical services or sensitive information to the cloud.

To address this, a recently released roadmap from the National Institute of Standards and Technology recommends a plan to ensure cloud offerings meet government security needs while being flexible enough to adapt to the policies and requirements of multiple tenants, including foreign governments. The plan involves periodic assessments of security controls and development of international profiles and standards.
The recommendations are brief and make up a small part of the 140-page document released by NIST in October but categorized as “high priority.”

The final version of the U.S. Government Cloud Computing Technology Roadmap has been several years in the making and reflects more than 200 comments on the initial draft, released in 2011.

Security is the first of three high-priority requirements addressed in volume one. Interoperability and portability — the ability of data to be moved from one cloud facility to another—are the others.

The government established FedRAMP, which became operational in 2012, to ensure that cloud service providers meet a baseline set of federal security requirements, easing the task of certifying and authorizing the systems for government operations. But the NIST roadmap addresses security requirements that extend beyond federal users.

Security in the cloud is complicated by a number of factors. First, it upsets the traditional IT security model that relies on logical and physical system boundaries. “The inherent characteristics of cloud computing make these boundaries more complex and render traditional security mechanisms less effective,” the roadmap says.

Second, a cloud system has to meet not only U.S. government security needs, but also those of other customers sharing the environment, and so security policy must be de-coupled from U.S. government-specific policies. “Mechanisms must be developed to allow differing policies to co-exist and be implemented with a high degree of confidence, irrespective of geographical location and sovereignty.”

Moreover, a comprehensive set of security requirements have not yet been fully established, the roadmap says. “Security controls need to be reexamined in the context of cloud architecture, scale, reliance on networking, outsourcing and shared resources,” the authors write. “For example, multi-tenancy is an inherent cloud characteristic that intuitively raises concern that one consumer may impact the operations or access data of other tenants running on the same cloud.”

NIST says recommended priority action plans for cloud security are:

- Continue to identify cloud consumer priority security requirements, on at least a quarterly basis.
- Periodically identify and assess the extent to which risk can be mitigated through existing and emerging security controls and guidance. Identify gaps and modify existing controls and monitoring capabilities.
- Develop neutral cloud security profiles, technical security attributes and test criteria.
- Define an international standards-based conformity assessment system approach.

**Critical Read**

**DOD guide looks beyond FedRAMP protections**


**WHY:** The unclassified guide, posted on the open-source Public Intelligence website, follows up on a Dec. 15 memo from the DOD CIO’s office that defines component agencies’ responsibilities when they acquire commercial cloud services, which include complying with the security requirements in the Federal Risk and Authorization Management Program and the new Cloud Computing SRG. The Defense Information Systems Agency had previously published guidelines for using commercial cloud products under the Cloud Security Model.

The SRG states that because of its warfighting mission, DOD has unique information protection requirements that extend beyond the capabilities assessed via FedRAMP. The new document outlines those security controls and additional requirements necessary for using cloud-based solutions within DOD.

The Cloud Computing SRG serves several purposes, including:

- Providing security requirements and guidance for non-DOD cloud providers that want to have their services included in the DOD’s catalog of cloud services.
- Establishing a basis that DOD will use to assess the security posture of a non-DOD provider’s cloud services.
- Defining the policies, requirements and architectures for using commercial cloud services within DOD.

**VERBATIM:** “Cloud computing enables the department to consolidate infrastructure, leverage commodity IT functions and eliminate functional redundancies while improving continuity of operations. The overall success of these initiatives depends upon well-executed security requirements, defined and understood by both DOD components and industry.”