FedRAMP Significant Change Request Form

Instructions:	1. Complete the form and attach additional pages if necessary. 2. Upload either a digitally signed copy or a physically signed and scanned copy to OMB MAX. 3. Send a notification message to info@fedramp.gov - include OMB MAX location of the document.

CSP Contact Information			
Company Name	U.S. General Services Administration, 18F		
System Name	cloud.gov		
System Owner	Carlo Costino	**Title**	Director of cloud.gov
Primary POC	Britta Gustafson	**Title**	Deputy director of cloud.gov
	[omitted]	**Email**	[omitted]

System Information	
Type of System	PaaS
Please briefly describe your system	18F built cloud.gov to help teams responsible for delivering federal digital services to operate those services efficiently and at-scale in a cloud-hosted environment while easing the burden of complying with federal requirements.
List current and pending Federal customers	ATF, Education, DOI, EPA, FBI, FDIC, FEC, Forest Service, GSA, IRS, OPM, OMB

3PAO Information (Required)		
3PAO Company Name		
3PAO Primary POC	**Name:**	**Title:**
	Phone:	**Email:**
Currently on contract for significant change proposed?	No	
Security Assessment Plan attached?	No	

Nature of Change	
Change Details – Please provide background and brief description *(attach additional pages if necessary):*	**Background:** cloud.gov currently relies on AWS Route 53 for DNS services because it supports the use of ALIAS records at the root of the domain. This allows us to use an AWS Elastic Load Balancer (ELB), which requires being addressed in DNS records by name, not IP, for the root https://cloud.gov URL.

For context on our current implementation, see SSP section 9.2.1:

> “Relatedly, managing DNS using AWS tooling significantly reduces the complexity of our operations. By using Route 53, we can fully automate our DNS setup, completely eliminating the risk posed by mistaken or accidental manual changes to the DNS configuration. Combined with the above services tracking the logs and configuration changes to DNS, we have achieved an extremely high level of continuous monitoring across all of our critical dependencies. Additional risk compensation in using Route 53 can be found below in control SC-20.”

SC-20:

> “By using and configuring AWS Route 53, cloud.gov combines DNS management with our HTTP Strict Transport Security (HSTS) endpoints to achieve data origin authentication and integrity verification along with the authoritative name resolution data the system returns in response to external name/address resolution queries.
>
> 18F does not implement DNSSEC. HTTPS serves as an alternative and compensating control, providing all of the same security assertions, and more. By implementing HTTPS in this fashion, any successful DNS poisoning would cause the system to fail into a "closed state" and throw an error in the browser, such that our systems could not be impersonated.”

SC-22:

> “cloud.gov implements Route 53 exclusively for external DNS services. Route 53 DNS utilizes multiple servers using weighted round-robin DNS. See https://aws.amazon.com/route53/ for further details.”

Description of the change:

We plan to replace AWS Route 53 with an in-boundary deployment of the open source PowerDNS product (https://www.powerdns.com/). PowerDNS, which we run for internal DNS resolution among our instances, has added recent features that allow us to not only to continue to use ALIAS records for our ELB references, but also has features that allow for flattening those records periodically to their IP address equivalent. This automatic flattening gives us the ability to implement DNSSEC as outlined in *OMB Memo M-08-23* for the cloud.gov domain.

This would affect our SSP in the following ways:

- We would update section 9.2.1 to remove all references to AWS Route 53, and our usage being out of the boundary and scope of review, since this would no longer apply to our implementation.
- We would update SC-20(a) to remove references to Route 53, and wording about not implementing DNSSEC, and our previous justifications. This would move this control to Implemented, without Alternative Implementation. New control description:

> **cloud.gov PaaS**
>
> By using and configuring PowerDNS and implementing DNSSEC for secure zone signing, cloud.gov combines DNS management with our HTTP Strict Transport Security (HSTS) endpoints to achieve data origin authentication and integrity verification, along with the cryptographically verifiable authoritative name resolution data the system returns in response to external name/address resolution queries.
>
> HTTPS and HSTS serves as an additional control, providing all of the same security assertions, and more. By implementing HTTPS in this fashion, any successful DNS poisoning would cause the system to fail into a "closed state" and throw an error in the browser, such that our systems could not be impersonated.
>
> **Customer Responsibility**

For customer applications, customers are responsible for selecting a name resolution service that fulfills this requirement and any requirements of their respective agency. cloud.gov requires HTTPS for all applications regardless of the name resolution service provided. See https://cloud.gov/docs/apps/custom-domains/ .

- We would update SC-22 to remove Route 53, and expand on our use of PowerDNS:

  cloud.gov DNS

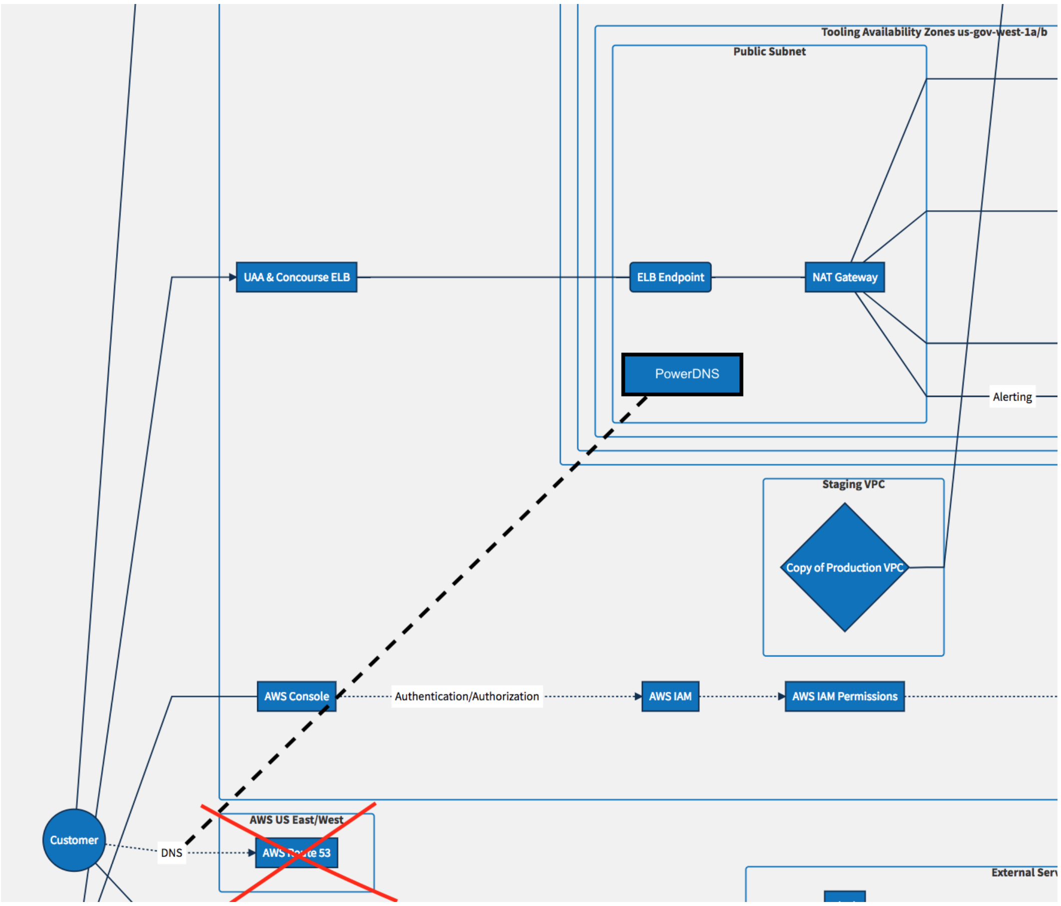
  cloud.gov implements PowerDNS for the cloud.gov domain using a highly available multi-server cluster available to the public internet. This cluster is maintained using our standard orchestration tool, BOSH. cloud.gov implements PowerDNS and Consul to resolve the names of internal Cloud Foundry components. These internal systems are not accessible from the internet.

  All systems are managed using our configuration management policy (https://cloud.gov/docs/ops/configuration-management/).

  Customer Responsibility

  Customers are responsible for managing their own DNS services. Public name resolution is not a service provided by cloud.gov.

- We would remove the mention of Route 53 from CP-9 (3). (*"Amazon Web Services (AWS) handles durability, availability and monitoring of some regional and global services (e.g. IAM, Cloud Front, Cloud Search, Dynamo DB, Amazon S3, and Route 53)."*)
- We would remove Route 53 from the Services Table attachment.
- We would update the SSP Roles table to remove references to TTS Infrastructure staff having "write access to DNS" since authoritative DNS records would fully live in a repository owned by cloud.gov Operations team.
- We would update the 10-1 Network diagram (https://diagrams.fr.cloud.gov/10-1-network.html) to remove the Route 53 component and add the in-boundary PowerDNS component.



Security impact assessment

We expect implementing DNSSEC for the cloud.gov domain will improve our risk posture, and improve our compliance with current Federal policy.

Our move from Route 53 to internal DNS will reduce our dependencies on external services outside of FedRAMP JAB Moderate boundaries, while still enabling us to continue to fully automate our DNS setup. We still consider our security implementation for SC-20 to primarily rely on our strong and strict implementation of HTTPS, with DNSSEC as an enhancement.

Generally use of the PowerDNS component itself does not change our risk posture, because we already use PowerDNS internally for resolution among our EC2 instances, as referenced in the current SC-22 description (*"Internally cloud.gov implements PowerDNS and Consul to resolve the names of internal cloud foundry components."*).

Additionally, PowerDNS has been a trusted product for supplying DNS services for almost 20 years, capturing almost 90% of the European market for DNSSEC implementations, and specifically developed the ALIAS flattening features for whitehouse.gov (https://blog.powerdns.com/2016/07/11/welcome-to-powerdns-4-0-0/).

This change also moves the DNS record data from one repository shared by all of 18F staff (https://github.com/18F/dns), to one completely within the control of the cloud.gov Cloud Ops team (https://github.com/18F/cg-deploy-powerdns).

Type of Change

Type of Change *(check all that apply):*	☐ Authentication or access control ☐ Storage ☐ New code release x Replacement of COTS product ☐ Change in services offered ☐ Change in FIPS 199 Categorization Level (Moderate to High requires Attachment A) ☐ Other (Please Specify): ☐ Backup mechanism or process ☐ SaaS or PaaS changing underlying provider ☐ Changing alternate or compensating control ☐ Removal of security control(s) ☐ Change in system scope
System Component(s) Impacted *(List all)*	Route 53 DNS
Security Control(s) Impacted *(List all)*	*Major impact:* SC-20 SC-22 *Minor impact:* CP-9 (3)
Has the 3PAO validated above control list?	No
Status of Change	In development
Is there a date by which this change must be operational?	No

<table>
<tr><td colspan="2"><b>Validation</b></td></tr>
<tr>
<td><b>Please describe how the impacted controls will be validated once the change is complete.</b>
<i>(attach additional pages if necessary)</i></td>
<td>

SC-20

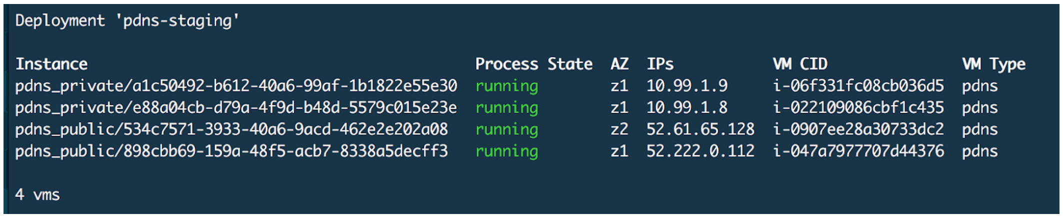
To validate that we have correctly implemented DNSSEC features as described in SC-20, anyone can use a third-party tool, such as the one from VeriSign (https://dnssec-debugger.verisignlabs.com/).

To validate that we continue to maintain our described implementation of HTTPS features (including HSTS), anyone can use a third-party tool, such as the one from Qualys (https://www.ssllabs.com/ssltest/index.html).

SC-22

To validate that we have implemented PowerDNS as described, we can provide screenshots (or an exported spreadsheet) of our component inventory, which is automatically maintained by BOSH. We can also provide our Nessus scans that include those components. The exported inventory and Nessus scans are part of our monthly Continuous Monitoring report, so that information can be validated continuously.

Example screenshot of PowerDNS test cluster instances in our staging environment, as seen from the BOSH orchestration tool:



```
Deployment 'pdns-staging'

Instance                                            Process State  AZ  IPs           VM CID               VM Type
pdns_private/a1c50492-b612-40a6-99af-1b1822e55e30  running        z1  10.99.1.9     i-06f331fc08cb036d5  pdns
pdns_private/e88a04cb-d79a-4f9d-b48d-5579c015e23e  running        z1  10.99.1.8     i-022109086cbf1c435  pdns
pdns_public/534c7571-3933-40a6-9acd-462e2e202a08   running        z2  52.61.65.128  i-0907ee28a30733dc2  pdns
pdns_public/898cbb69-159a-48f5-acb7-8338a5decff3   running        z1  52.222.0.112  i-047a7977707d44376  pdns

4 vms
```

</td>
</tr>
</table>

	Our deployment configuration is publicly available at https://github.com/18F/cg-deploy-powerdns . A person with access to our inventory and scans can verify that the configuration (such as the number of instances in the cluster) matches the inventory and scans. Anyone can also validate that this component follows our Configuration Management Plan (https://cloud.gov/docs/ops/configuration-management/), including: maintained in version control, managed by BOSH, and tested and deployed by Concourse pipelines. **CP-9 (3)** No validation needed, as this was a brief mention.
Demand/Justification	
Which customers are driving this change? *(Always required for changes to service, scope, or FIPS- 199 Level)*	[omitted]
Justification for change. *(attach additional pages if necessary)*	[omitted] does not accept our alternative implementation for SC-20. For [omitted] customer system ATOs, [omitted] requires us to implement the OMB M-08-23 mandate for DNSSEC (https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2008/m08-23.pdf) for the cloud.gov domain and subdomains.
Is the change required because a previous version is reaching end of life or end of support?	No
Is this change intended to enhance ConMon performance?	No
CSP Signature *(To be signed by an individual with the authority to represent the CSP to FedRAMP)*	
Name *(Type)*: Britta Gustafson	**Title:** Deputy director of cloud.gov
________________________________ **Signature**	________________________________ **Date**
FedRAMP Standing (to be Completed by FedRAMP)	
Annual Assessment	
Was the last Assessment Completed?	Yes / No
When is the next Annual Assessment Due?	

Is CSP currently overdue on its Annual Assessment?	Yes / No If Yes, why:
ConMon Performance	
Was CSP on a corrective action plan in the past six months?	Yes / No
For FedRAMP PMO Use Only	
Approved: Yes / No	**Date:**
FedRAMP Reviewer's Name:	
FedRAMP Reviewer's Notes *(Optional)*	