



Connect.Gov Request for Information (RFI) – Industry Day Questions and Answers

Date: June 2, 2015, 1:00PM Eastern

The following questions were received during the Connect.Gov Industry Day webinar. The responses provided include the responses provided during the session, as well as additional information provided by GSA.

Questions & Answers

1. Will the Request for Information (RFI) result in a Request for Proposal (RFP) being issued?

Every time GSA issues an RFI, specific language is included stating that this document is not an RFP and therefore, the information is used as market research and information for planning purposes only. It does not constitute a solicitation for bids, proposals for quotations. Based on the information received, the government will determine if an RFP will be issued in the future.

2. Will the webinar be recorded and made available?

The session is being recorded but will not be made available. However, the slides and Q&A discussed during the session will be shared with the public and posted on [FedBizOpps](#) on the RFI and Industry Day postings as well as [GSA Interact](#).

3. How do you plan to educate users about the benefits of Connect.Gov services?

GSA is working with Agencies, who know their customers well and have established marketing channels to help market the capabilities of using another credential, rather than an agency-specific one, for use across government applications. GSA is also working very closely with NSTIC who has extensive experience in private sector outreach. Market campaigns and educational outreach will be conducted. GSA recently published a video on the [Program website](#). GSA is in the early stages and recognizes this is a change in user behavior. Consumers are now very familiar with using Facebook and Google to launch other applications but they also know it may be used to track that information. The power of the Connect.Gov platform is it will prevent tracking of personal information, enabling a more secure and private experience. We recognize we need a marketing campaign to spread that word.

4. Can you provide a list of Agency services that will use Connect.Gov in the next 3 months at (Level of Assurance) LOA2 and above and the number of users per year of service?

VA, State Dept., USDA and HHS are all evaluating LOA 2 applications.

5. Can you provide more information about USPS' role as the technology service provider for Connect.Gov?

GSA is working with the United States Postal Service (USPS) who operates the secure, cloud-based hub that adheres to strict privacy and security standards. SecureKey currently has the contract to



provide the broker hub service. They also provide integration support, working with agencies and credential service providers (CSPs). Verizon and ID.me have contracts with GSA to provide credentialing services under the Connect.Gov Program.

6. Will Connect.Gov manage federation between CSPs and applications?

Yes. The Connect.Gov system provides a federated hub from which CSPs and government Agencies integrate into the cloud-based hub.

7. How will anticipated changes to NIST SP800-63-2 impact the Connect.Gov initiative?

[NIST SP 800-63 Rev 2](#) is reflected in the Federal Identity Credentialing and Access Management (FICAM) Trust Framework Provider (TFP) adoption process. CSPs that are certified as FICAM compliant are conforming to NIST SP800-63-2 as they are reflected through FICAM. The Connect.Gov program adheres to 800-63 and leverages identity providers that comply with FICAM.

8. Who are the contractors involved in the Connect.Gov program?

SecureKey provides the broker hub service for Connect.Gov. GSA has contract with two FICAM approved CSPs - Verizon & ID.me

9. Will this be a small business set aside?

The acquisition strategy has yet to be developed but that is an option which will be considered so long as there is a sufficient vendor pool which meets all program requirements and standards.

10. Will existing CSPs be able to provide credentials which can elevate to different Levels of Assurance (LOA)s?

Credential providers who provide LOA2 and LOA3 can provide LOA1. LOA1 CSPs who meet FICAM requirements and are approved should be able to provide services for LOA2 and LOA3 in the next bid.

11. If a different, but acceptable technical solution exists in the marketplace, is the government willing to adopt it and replace the current IOC solution?

Yes, GSA will entertain all options based on the evaluation of solutions against program requirements.

12. Is the intent to move the existing hub to the cloud and have a contractor operate it?

The existing hub is already a cloud-hosted solution and is provided by the contractor SecureKey.

13. If this does go to RFP, will the contract be issued by USPS or GSA?

GSA will be issuing a contract(s) if it goes to RFP.

14. Has there been consideration for USPS for in-person proofing?

GSA, along with partners at USPS, is exploring all options for in-person proofing capabilities.



15. Will Blanket Purchase Agreements (BPAs) be restricted to Schedule70 or will they also be available in other vehicles?

GSA will examine the solutions available under various acquisition vehicles and based on the available competition, among other factors, will determine the best acquisition solution.

16. Do GSA client Agencies really want or need this service?

GSA sees increasing demand among Agencies for this type of solution. As more agencies are looking to deliver online services to citizens, the need for privacy-enhancing credential services will only continue to grow.

17. How is the U.S. Department of Veteran Affairs (VA) utilizing Connect.Gov?

The VA is looking to integrate six different applications to allow its user base to sign in with Connect.Gov.

18. Is there an expected timeframe for Connect.Gov hub to go live?

The Connect.Gov program is live today with many different Agencies rolling it out in various stages of implementation.

19. What vendor is providing the existing cloud-based hub?

SecureKey.

20. Is Connect.Gov being used to fulfill the October 2014 Presidential Executive Order and if so, what's the timeline for that? The original timeline was to be March 2016.

The Connect.Gov Program meets the requirements outlined in the 2014 Executive Order but we are still waiting for the implementation guideline to find out how the program can help meet the requirements.

21. Will the acquisition be a single or multiple award?

The approach remains to be determined. GSA is looking at both options/strategies and looks forward to hearing Industry input for suggestions and readiness to support either or all models.

22. Other than the Agencies listed earlier in the presentation, what other agencies are expected to participate on Connect.Gov?

GSA is talking to multiple Agencies and components of Agencies but the ones in the presentation were the ones who are far enough along and willing to lend their names to the program.

23. Are we required to use SAML, Oauth, or OpenID?

The Connect.Gov Program uses Security Assertion Markup Language (SAML) 2.0 to communicate from the hub to an agency and SAML 2.0, OpenID, and OpenID Connect between the broker and CSPs. GSA is working with the National Institute of Standards and Technology (NIST) and others on an OpenID connect profile that may be used between Agencies and the broker.

24. Do client agencies fund their own effort to integrate to the hub to consume Connect.Gov credentials?

Yes, client Agencies will fund their own integration efforts. The Connect.Gov Program works closely with Agencies helping them integrate their systems to the secure Cloud hub.



25. As the broker for credentials, what type of monitoring will Connect.Gov provide?

The Connect.Gov hub is a FedRAMP compliant solution with multiple layers of security defenses.

26. Is Connect.Gov live and working today and if so, why are we considering a new system?

The system is live and working today. GSA is asking Industry for ideas on how the government can best procure services that make the most sense for government and citizens alike. The RFI outlines two different operating models on how to acquire these services and GSA is very interested to hear Industry's perspective on which one might be most effective. GSA has been interacting regularly with different Agencies that are eager to move towards a shared service model and want to make sure the Connect.Gov Program meet the needs of Agencies as well as industry partners and the public.

27. What controls and monitoring will be employed to ensure user-credential privacy? Who will be responsible for monitoring services?

GSA has worked extensively on Connect.Gov privacy features to maintain the privacy of all users. The main privacy-enabling feature, known as blinding, prevents CSPs from tracking or building personal profiles of any user across the platform. CSPs do not know the Agency endpoint of any user and Relying Parties (RPs) do not know the CSP that originated the request. Additionally, the broker does not store any personal information that is transmitted. GSA also continues to conduct R&D in implementing state-of-the-art features to protect privacy and security.

28. Will Connect.Gov utilize tracking cookies to monitor activities and changes in data?

No, the government does not use tracking cookies within Connect.Gov to monitor any user activity. The broker has information about the session and uses unique, but meaningless, identifiers to ensure the credential is directed to the appropriate agency.

29. After June 19, will there be an open discussion period between GSA and vendors to discuss responses to the RFI?

Yes, GSA will analyze the responses and look for interesting ideas and themes, and may reach out to different respondents for one-on-one discussions.

30. Will the government track a users' credential across the platform?

A broker maintains an understanding of the unique identifier related to the user credential but does not know who the user is – because they do not store any personal information and will be directed to the appropriate agency.

31. Using Google ID on Connect.Gov does not ensure full security since it does not require multi-factor authentication. How does Connect.Gov plan to address this issue?

In the Connect.Gov platform, Google ID is only allowed for LOA1 transactions, for systems which require no level of assurance. The decision on what LOA is required is based on each application's requirements. Any application that requires multi-factor authentication will not be able to use LOA1 credentials.

32. Is the government interested in multifactor authentication, possibly to include biometrics?

Yes, CSPs are certified under FICAM which conforms to NIST SP 800-63 rev 2.



33. When do you expect to start allowing component identity services to integrate with Connect.Gov?

GSA is still looking at component identity services with NIST, FICAM and other groups. Once GSA has assessed the situation, the team will see what the capabilities are to integrate into the Connect.Gov platform.

34. What is the vision of the long-term role for USPS on the Connect.Gov portal?

USPS is a strategic partner and a trusted entity, with a unique digital services offering and a large footprint. They will continue to provide great value and be a partner in the Program.

35. Are there performance metrics for the current activities on the portal?

Metrics collected to measure performance on the portal exist but will not be shared at this time.

36. Will existing CSPs be permitted to bid on the contract?

Yes, GSA anticipates that CSPs will be permitted to bid on future contracts for the Connect.Gov program.

37. If GSA adopts operating model 2, how would a contract allow the broker to pay fees to GSA?

Agencies will be able to issue Task Orders against the BPA from which fees would be covered. Please refer to the RFI for more information on how services would be remitted to GSA.

38. Do you see a role for smartphone authentication in the Connect.Gov process? Is this a focus for Connect.Gov or just a sideline?

The goal of the NSTIC is to have a variety of authentication methods so users can have a choice. CSP authentication methods must be FICAM certified.

39. Are derived credentials on the horizon for Connect.Gov?

The Connect.Gov Program is looking into derived credentials.

40. Will service providers be paid monthly, weekly, daily, for the amounts of services they provide users and agencies?

GSA anticipates monthly payment bill cycles.

41. Please provide some insight into issues the program is experiencing – it would help to guide us in providing feedback.

- a) As there are several contracts, it is challenging to get a centralized view of all activities.
- b) GSA is looking for opportunities on multi-factor authentication and opportunities for agencies to have higher levels of assurance/security than currently offered.

42. Are you aware of other countries that have already implemented a government-run ID authentication system? If yes, have their experiences been included in the current modeling?

GSA is engaging with other countries (e.g. Canada, the United Kingdom) to exchange ideas about government-run ID authentication systems.