Question	Answer
For each of the systems, how many system interconnections are there?	Information about individual systems is considered sensitive. Systems have, on average, between 2 and 4 interconnections.
For each of the systems, how much (% wise) of the system controls are inherited from one or more systems are not contained within the authorization boundary of the system and do not necessarily exist in the system's environment of operation?	Information about individual systems is considered sensitive. Varying somewhat by system, approximately 40%-60% of controls are inherited from a cloud or common control provider. The common control provider system does not fall into this category.
Do all of the systems providing common (i.e., inherited) controls (e.g. any type of service or functionality used such as identification and authentication services, network services, or monitoring functionality) for other systems have an ATO? If not, are these provider systems included in this group of new systems up for ATOs?	The system providing common controls has not yet been accredited. It is included in the list of new systems requiring an ATO.
Will the General Support System (GSS) be among the systems assessed and received ATO? If so, is the GSS's function as a provider for other systems in scope?	Yes it will be assessed. Yes, it is in scope for the systems that inherit controls from the GSS.
How many of the systems handle PII? Of those with PII, how many of them have associated SORNs (system of record notices)?	There are currently two systems that handle PII (although others have sensitive information of a financial or business sensitive nature). Both of these sytems fall under a SORN.
Is the RMF integrated to have security and privacy requirements and controls into enterprise architecture, system development life cycle (SDLC), acquisition processes (e.g. supply chain), and systems engineering processes?	Programs to ensure that RMF is integrated throughout our processes are being formalized at this time. Although not fully formal, there are processes in place to support RMF throughout the organization.
How many of the systems include security considerations as guided by NIST SP 800-64 and 800-160 v1?	USAC systems are developed/engineered with security considerations in mind.
Are the development environments, systems undergoing modifications and upgrades, and systems under development included with an identified authorized system or one to obtain ATO?	Yes, all USAC systems requiring authorization/continuous monitoring, including those undergoing changes, have been included within those listed in the RFP.
Have development environments been assessed concurrently with the production environments or are they assessed separately?	Currently the assessments are solely being conducted on production environments.
How many systems are considered common control providers?	One system is considered a common control provider.
How many common control providers currently have ATO?	The common control system does not have an ATO.
How many of the systems are internal use only vs. externally facing?	3 systems are internal facing and 7 are externally facing.
What is the maturity level of the documentation for these systems?	This is not relevant for this RFP.

Is it USAC’s desire to conduct the assessment of these systems as a single-pass evaluation of system state, or does it desire intermediate feedback and chance for remediation prior to release of the Security Assessment Report (SAR)? If more than a single-pass evaluation is desired, how many passes is USAC desiring and will the number of passes be considered for any slippage on dates if it bypasses critical path of the project plan?	A multi-pass method may be required and consideration of date slippage will the taken into account. A system by system determination will need to be made.
Have any of the systems previously been denied an ATO?	No.
Are project deadlines negotiable based on dependencies and critical paths/deliverable/documentations precursor deadlines?	Most USAC systems have hard dates based on requirements/deadlines implemented by the FCC. However, project deadlines will be established with a reasonable expectation for the successful completion of required assessment activities.
Of the common controls identified as being leveraged by USAC individual systems, how many have been evaluated to ensure that inheritance is provided in the intended and secure manner? For each of those systems, how many controls are leveraged that must be assessed?	The (one) common controls provider is currently requiring ATO. This process will ensure that inheritance is provided in the intended and secure manner.
The milestone due dates in Table 3 of the solicitation suggest that systems are slated to be assessed concurrently. Can USAC confirm that the expectation is for concurrent reviews of systems?	Confirmed. The expectation is that systems will be assessed concurrently.
Are all common controls covered by approved system security plans and possess current authorizations? How many of those controls will be assessed as part of ISCM?	The (one) common controls provider is currently requiring ATO. The ongoing ISCM assessment of controls is established in our ISCM plan with the key controls and annual 1/3 controls defined.
How many completed POA&M items must be assessed per system each year?	Irrelevant for the work required by RFP.
How many POA&M items are considered common controls?	Irrelevant for the work required by RFP.
Based on section A:I. Overview of Project, there is mentioning of initial ATO for up to 4 systems per year for 2019-2021; however, on the Attachment 1-Bid Sheet, pricing is only asked for 2 ATOs for base year, 3 for option year 1, and 0 for option year 2? Will there be provisions to modify pricing and scope for up to the 4 systems mentioned per year (for potentially a total of 12 systems)?	The total number of systems currently projected is 10 over the course of all 4 option years. The total number of systems is 8 for CY 2019.
Section B:V. Performance Requirements states that the project plan must be submitted to the USAC IT Security Director for approval AND that Contractor shall begin performance of Security Controls Assessment tasks no later than ten (10) business days following the project kick-off meeting. Will USAC consider modifying the terms to having the tasks begin no later than ten (10) business days following project plan approval?	This is acceptable.
Based on the Attachment 1-Bid Sheet, are the 5 ATO systems (2 for base year and 3 for option year 1) included as part of the systems undergoing ISCM the year after ATO is received? If so, is there a provision allowed to modify the number of systems from 10 systems identified in options year 2 to 11 systems (6 systems in based year + 5 ATOs from based year and option year 1)?	The total number of systems currently projected is 10 over the course of all 4 option years. The total number of systems is 8 for CY 2019. The 3rd ATO for option year 2020 is a projected re-authorization based on major system changes for a system that already has an ATO.

Section B:VI.B.5 asks for the contractor to "develop a Continuous Monitoring Security Controls Assessment Plan and Schedule." However, Section A.I states that "[ISCM assessments] will be in line with the USAC CM plan with the annual 1/3 controls and key controls." Can USAC clarify on what the expectation is for the contractor-developed CM assessment plan? Should the contractor's CM assessment plan be a SAP aligned to the ISCM policy and program which includes USAC's desire for annual 1/3 controls and key controls; or will the contractor be allowed to recommend best security goals and targets for assessment, PenTesting, etc. under CM?	USAC's ISCM policy and plan should be followed. Feedback on process improvement will be welcomed by USAC and implemented only at USAC's discretion.
There is no size, scope, complexity, or FISMA categorization provided for the listed systems. Can USAC please provide this information so that we can accurately assess the level of effort needed to support the requirements?	All USAC systems are categorized at a Moderate baseline. The size, scope, and complexity of the assessment should be based on this baseline (287 controls, with the additional privacy controls for those systems with PII).
Is Attachment 2 a Government-provided attachment?	No, resumes should be provided by the bidder as Attachment 2
In which section shall a risk mitigation plan be provided?	As stated in the RFP, this is part of RMF Task 4.3 (TASK 1.3) – Security Assessment Report.
What is anticipated to be the primary work location?	Please refer to Section B.IV.A
If the primary place of performance is contractor facilities and site-visits are required to complete assessment and ongoing monitoring duties, will that travel be reimbursable?	Please refer to Section B.II
Who is the Authorizing Official that our assessments will be informing and for what organization or Agency to they work?	The Authorizing Official is the USAC CIO. This person is a USAC employee. All USAC ATO packages are reviewed by the FCC.
Per page 46, section 8.a, please define the phrase "peer advisor"?	This is a typographical error. The required information is for "security controls assessors"
Are tables of contents counted in the page counts?	No table of contents is requied and will subsequently count against the page count.
Is this an initial assessment, if not, who was the previous incumbent?	This information regarding a previous USAC vendor is considered sensitive.
Can you please provide the name of the vendor who performed the RMF Steps 1-3?	No.

In Table 3, USAC SCA Milestone Timetable, Task Activity "ATO" is described. What does this entail? Is this an update of the required SA&A package documentation, or does this also require the review of all system controls? Please elaborate.	Please refer to the RFP. This procurement is explicitly for the "USAC SECURITY CONTROLS ASSESSMENT EFFORT".
Page 44, Section B.3; "in-depth discussion of Offeror's technical approach to providing the services listed in Section B.VI.," and page 45, Section B.7 Timeline; "describe in detail their process for conducting activities to manage the SCA, including how the Offeror intends to staff and complete related activities. Offerors shall describe in detail their plan for completing the services as identified in Section B.V and Section B.VI. in a time allotted" This language seems redundant. Can USAC please clarify if the intent is for the offeror to provide a detailed approach and process for both the technical approach and the timeline sections? Will USAC prefer a detailed explanation of approach and process in the technical section, and a separate timeline that corresponds to the technical approach, or does the government want equal detail of approach and process in the technical as well as the timeline sections?	This is somewhat redundant. However, one section refers to the details about the process and the other to the detailed timeline.
What is USAC's budget for this project?	USAC does not share budgetary information.
Are both internal and external networks in scope for vulnerability testing? a. If so, what is the approximate number of active internal and external IPs, respectively?	USAC conducts vulnerability test on all applicable IP's. This information will be available to the SCA vendor for the appropriate assessment of relevant controls.
The RFP states that vulnerability and penetration testing reports might be applicable deliverables. Does USAC require penetration testing for internal and/or external networks?	USAC procures a separate independent resource to perform a penetration test on the systems. This is not relevant to this RFP.
Does USAC require vulnerability and/or penetration testing of web applications? a. If so, what is the number of URLs to be tested? b. How many applications are in scope?	USAC procures a separate independent resource to perform a penetration test on the systems. This is not relevant to this RFP.
Are configuration reviews in scope (i.e., firewalls, servers, database, workstations, routers/switches)? If so, please provide the number of: a. Firewalls and if any firewalls are in HA pairs. b. Server operating systems and their versions. c. Database operating systems and their versions. d. Workstations in scope. e. Routers/switches in scope.	Verification that controls related to these items are in place. The specific configurations of USAC systems is considered sensitive information and will be provided upon vendor selection. USAC IT is a medium sized environment with approximately 2k servers and 1000 employees and contractors.
Would USAC like to see resumes in section 6 of volume II or section 8 of volume II?	Purusant to Section B.E.V, resumes should be submitted as Attachment 2 to Volume II.
RFP Section D: Attachments lists an Attachment 2 for Resumes. Item 8 in B. Technical (Volume II) says to attach resumes as Attachment 3. Could USAC confirm there are only two attachments for this RFP, including the bid form and resumes?	Confirmed.
Can USAC explain the quantities listed on Attachment 1? These numbers do not match the systems listed in Section A. I. Overview of the Project. Is the ATO line for services that fall under NIST RMF Step 4 and the ISCM line for services under Step 6?	Correct.

There are two locations in the RFP that contain the scope of the assessments. In the last paragraph of Section 1. Overview of the Project there are details of the number of ATOs and 1/3 control reviews for the years 2019-2021. Also, Table 3 Milestone Table contains a list of the assessments required for the years 2019-2023. We were not able to reconcile these two. For instance, section 1 states there are 4 SCAs for ATO in 2019 and 6 1/3 control reviews. For this same time period, Table 3 states there are 2 ATOs and 6 1/3 control reviews.	This is an incorrect statement. Section A.1 refers to the possibility of up to 4; however, Section B.V.C Table 3 gives a clear timeline for the project.
Table 3 and the bid sheet have the abbreviation ISCM, Information Security Continuous Monitoring Program. Is our understanding correct that ISCM would mean 1/3 control review and ATO would mean a full control review? If not, can you please explain the difference?	The understanding expressed here is accurate. ATO refers to to full control review. ISCM refers to key controls plus 1/3 controls review.
If there is an existing incumbent, what size are they?	No
Is this requirement being set-aside for a Small Business?	No
Does USAC want or require a Table of Contents for each volume?	No table of contents is requied and will subsequently count against the page count.
What is meant that "If there Contractor shall provide the resumes/biographies of three (3) sample executive peer advisors"?	It is unclear what section this is in reference to
What FISMA levels (low, moderate, high) is the systems for the ISCM and ATO task activities?	All USAC systems are at a FISMA level Moderate.
Does USAC have a GRC tool (i.e., Xacta; CSAM, etc) implemented? If not, where is security documentation/artifacts stored?	USAC does not currently have a GRC tool. Currently the artifacts are managed via collaboration tools.
Are any of the systems requiring assessment GCC's?	Question not understood. What does GCC stand for?
How many systems are Major Applications?	All systems requiring authorization are comprised of/include major applications.
Do any systems reside in a FedRAMP or third party vendor's cloud environment? If so in a FedRAMP environment, is the FISMA level for the FedRAMP systems?	2 of the USAC systems are with cloud vendors. Both of these vendors are FedRamp certified.
The due date for the ISCM and ATO task activities go out to Sep 30, 2019 is it expected that additional systems will be assigned for ISCM and ATO support after Sept 30? If so, what would be the expected mixture of ISCM and ATO systems to be assigned after Sep 30?	As stated in the RFP, for FY 2019, the ATO/ISCM activities run through October 15, 2019.
How soon after the projected start of the contract (i.e., 6/3) will the two (2) ATO Assessment (Step 4) task activity expected to begin?	Per the RFP work is expected to begin within 10 business days of kickoff.
Does USAC have their own Nessus instance that the contractor will use?	USAC does have their own Nessus instance managed by the USAC SOC team. Information from the tool will be made available to the contractor.
When was the last FISMA system Audit?	FISMA system audit runs from April-October every year.
Is there another USAC vendor responsible for supporting the RMF Steps 1 – 3 and 5 for the USAC systems?	Yes
Under the USAC Continuous Monitoring policy, is expected that all controls (technical, management, and operational) are assessed every year or just a subset?	ATO refers to to full control review. ISCM refers to key controls plus 1/3 controls review.

Pg. 19, Table 3, first two line items indicate due dates for Milestones 3 systems ISCM due June 30, 2019 and 1 system ISCM due July 31, 2019. However, on pg. 42, Section C, date work begins is indicated as 6/3/2019. On pg 7 section V., SCA is indicated as starting 10 days after project kick-off meeting. Pg. 21. Section VII. A. 1. i. indicates the kick-off meeting is within 5 days after contract award. , leaving only 1 weeks for testing and report for 3 systems. Award date 6/3/2019 + 5 days for Kick-off meeting = 6/10/2019 (assuming business days). 6/10/19 + 10 days for SCA to start = 6/24/2019. SCA starting on 6/24/2019 would not yield a completion date for 3 systems by 6/30/2019. CAN USAC extend that date to 7/31/2019?	Due dates of immediate deliverables will be discussed/extended based on the completion of vendors selection.
Pg. 20, Last par. Section C, All deliverables shall be placed in the SharePoint site. Are contractor systems connected to the SharePoint site to put the deliverables there or is the contractor using USAC computers to place the deliverables in the SharePoint site?	Contractor will place deliverable in the USAC extranet site which will be made available to the contractor.
Per Section V. Proposal Content, each volume must include a cover page as outlined in IV. Proposal Volumes Cover Page. The RFP-Security-Controls-Assessment, front cover sheet/page requires Offeror contact information and signature. How is this page to be incorporated to ensure compliance with instructions and page limit(s)?	Please follow instructions pursuant to Section E.V
Because proposals received that exceeds page count it is important to know font type and size. What is the requirement for font type and size?	There are no limits imposed for font type and size. Please keep in mind, the proposal must be legible or may be subject to Section E.VI.B: Down Select Process.
Due to the level of detail requested for past performance, please consider increasing the page limit from four (4) to seven (7) pages.	USAC rejects this request.
Will USAC only be implementing controls from NIST 800-53 or will it also be bringing in controls from other sources such as FISCAM, CIS, SOX, etc.?	Only controls from FISMA 800-53 are currently selected for USAC systems.
NIST 800-37 Rev 2 came out in December, 2018, but has not yet been adopted by most organizations. Will USAC be migrating to this standard during the course of this contract?	Yes.
NIST 800-53 Rev 5 will come out during 2019, but will not be widely adopted by most organizations for some time. Will USAC be migrating to NIST 800-53 Rev 5 during the course of this contract?	Yes.
Will USAC be providing a privileged account for running Nessus scans or will we have to coordinate with system owners for privileged access for each assessment?	USAC has their own Nessus instance managed by the USAC SOC team. Information from the tool will be made available to the contractor.
Does USAC already have a preferred SAR and SAP format or will the contractor be developing one with USAC?	One will be developed in conjunction with USAC Information security team.
What types of penetration testing may be applicable to these USAC systems?	This is not relevant for this RFP.
The number of systems in Base Year totals 8 systems (6 ISCM and 2 New ATO) however the Option Year 1 total systems in ISCM is only stated as 7 systems. Should this be 8 and the systems in ISCM for Option Year 2, 3,4 should total 11?	The total number of systems currently projected is 10 over the course of all 4 option years. The total number of systems is 8 for CY 2019. The 3rd ATO for option year 2020 is a projected re-authorization based on major system changes for a system that already has an ATO.

Systems are stated as Moderate Sized is this the size of the system or the system security level?	This is the security level based on FISMA moderate baseline.
Will the contractor be required to use their own tools such as Nessus or will we be using the USAC provided tools for assessment?	USAC has their own Nessus instance managed by the USAC SOC team. Information from the tool will be made available to the contractor.
Would USAC consider revising the initial inquiry timeline from 1 hour to a couple of hours since personnel may be in meetings when the inquiry comes in and not able to respond in that timeline.	This is acceptable.
This section only states Management, Operational and Technical Controls. Does the scope of work include assessing Privacy controls?	Yes, if applicable. (Question is understood and answered but it is unclear what section it refers to)
Is this considered to be a deliverable for the Assessment Documentation mentioned in Table2, USAC SCA Deliverables?	Unclear what "this" refers to.