

<b>AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT</b>				1. CONTRACT ID CODE		PAGE OF PAGES	
2. AMENDMENT/MODIFICATION NUMBER 001		3. EFFECTIVE DATE 08/01/2018		4. REQUISITION/PURCHASE REQUISITION NUMBER TCTOA-18-0013		5. PROJECT NUMBER (If applicable)	
6. ISSUED BY General Services Administration Federal Acquisition Service Technology Transformation Services 1800 F St NW   Washington, DC   20405		CODE		7. ADMINISTERED BY (If other than Item 6)		CODE	
8. NAME AND ADDRESS OF CONTRACTOR (Number, street, county, State and ZIP Code)				(X)		9A. AMENDMENT OF SOLICITATION NUMBER	
				<input type="checkbox"/>		TCTOA-18-0013	
				<input type="checkbox"/>		9B. DATED (SEE ITEM 11) 07/24/2018	
						10A. MODIFICATION OF CONTRACT/ORDER NUMBER	
CODE				FACILITY CODE		10B. DATED (SEE ITEM 13)	

**11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS**

☐ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended. ☐ is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:

(a) By completing items 8 and 15, and returning \_\_\_\_\_ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or electronic communication which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by letter or electronic communication, provided each letter or electronic communication makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

**13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS.  
IT MODIFIES THE CONTRACT/ORDER NUMBER AS DESCRIBED IN ITEM 14.**

CHECK ONE	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NUMBER IN ITEM 10A.
<input type="checkbox"/>	
<input type="checkbox"/>	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation data, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
<input type="checkbox"/>	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
<input type="checkbox"/>	D. OTHER (Specify type of modification and authority)

**E. IMPORTANT:** Contractor ☐ is not ☐ is required to sign this document and return \_\_\_\_\_ copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

TCTOA-18-0013 is hereby amended to incorporated the attached questions and answers. All other terms and conditions apply.

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)	
15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED
(Signature of person authorized to sign)		(Signature of Contracting Officer)	

# **General Services Administration**

Federal Acquisition Service

Technology Transformation Services

1800 F St NW | Washington, DC | 20405

# **Questions and Answers**

**Bug Bounty 2**

**TCTOA-18-0013 Amendment 001**

## **Contents**

[Issue #38](#)

[Issue #37](#)

[Issue #36](#)

[Issue #35](#)

[Issue #34](#)

[Issue #33](#)

[Issue #32](#)

[Issue #31](#)

[Issue #30](#)

[Issue #29](#)

[Issue #28](#)

[Issue #27](#)

[Issue #26](#)

[Issue #25](#)

[Issue #24](#)

[Issue #23](#)

[Issue #22](#)

[Issue #21](#)

[Issue #20](#)

[Issue #18](#)

[Issue #17](#)

[Issue #16](#)

---

## Issue #38

- [GitHub link](#)
  - Section of the RFQ
    - [RFQ Section 12 - Addendum - Commercial Contract Clauses](#)
    - The Commercial Contract Clauses document calls for the vendor to obtain FedRamp certification for their platform.
  - Question
    - Can the government confirm the type of certification that is expected (i.e. PaaS, SaaS)?
    - Is it the intent of the government to sponsor the vendor in their certification?
    - Is there any other support provided by the Government for the vendor throughout this process?
  - Answer
    - As is indicated in the RFQ section 12 Clause Addendum, FedRAMP Tailored or a FedRAMP Low assessment would be sufficient. A FedRAMP Moderate or High assessment would qualify, but is not necessary. GSA will sponsor the vendor for a FedRAMP Tailored certification, which involves working with the vendor to assist in the FedRAMP process. For more information about FedRAMP Tailored, please see <https://tailored.fedramp.gov/>.
-

## Issue #37

- [GitHub link](#)
  - Section of the RFQ
    - [RFQ Section 12 - QASP - Section 2.4](#)
    - It states “This document specifies all contractor key personnel, employees, and subcontractors shall execute the attached non-disclosure statement.”
  - Question
    - If the vendor already requires all participants to sign their own Non-Disclosure Agreement can this be used in-lieu of the Government NDA from a government review of the vendors NDA?
    - Can the government please identify where to find the Government NDA?
  - Answer
    - The government will provide an NDA to the awardee. The NDA must be signed by the vendor’s Key Personnel during or shortly after the kickoff meeting.
- 

## Issue #36

- [GitHub link](#)
  - Section of the RFQ
    - [RFQ Section 12 - Addendum - Commercial Contract Clauses](#)
    - Commercial Contract Clauses - it states reviewing the GSA IT Security Procedural Guide 17-75.
  - Question
    - Can the vendor have the GSA IT Security Procedural Guide 17-75 disclosed prior to the RFQ submission for review?
  - Answer
    - Upon request, TTS will provide GSA IT Security Procedural Guide 17-75 to offerors for review/reference.
-

## Issue #35

- [GitHub link](#)
  - Section of the RFQ
    - [RFQ Section 5.2. - Phase 2 Price Evaluation](#)
    - It states “Evaluation of options under FAR 52.217-8” Within FAR 52.217-8, in section 52.212-5(e)”
  - Question
    - Are the flow-down FAR clauses set forth under 52.212-5(e) apply to the researchers participating in the bug bounty research project?
  - Answer
    - If the security researchers are not under a subcontract with the platform provider for purposes of this acquisition, then the clause does not flow down.
- 

## Issue #34

- [GitHub link](#)
  - Section of the RFQ
    - [RFQ Section 5.2. - Phase 2 Price Evaluation](#)
    - It states “Evaluation of options under FAR 52.217-8” Within FAR 52.217-8, in section 52.212-5.
  - Question
    - Is the Contractor required to comply with the FAR clauses set forth under 52.212-5(e)?
    - Has 52.212-5 been constructed that as Contractor we need to comply with the FAR clauses listed in 52.212-5(a)-(d)?
    - Does the FAR clauses listed under 52.212-5(e) have the requirements for any subcontractors that are appointed?
  - Answer
    - FAR Clause 52.212-5 sections (a)-(e) all apply. FAR Clause 52.212-5(e) is specific to subcontractor requirements.
-

## Issue #33

- [GitHub link](#)
  - Section of the RFQ
    - [RFQ Section 5.2. - Phase 2 Price Evaluation](#)
    - It states “Prices shall be submitted via the Price Evaluation Form” there is a link to the price evaluation form.
  - Question
    - How can vendors get access to this page? When you click on it you receive the following message: "You can't respond to RFQ Pricing Response Form - Bug Bounty because you don't have permission to share documents outside of your domain. Contact your domain administrator if you think this is a mistake”.
  - Answer
    - The government has tested the pricing form as well as the upload capability on a non-GSA network with a non-GSA email and had no issue. Please contact your organization's IT department, as the problem seems to be localized.
- 

## Issue #32

- [GitHub link](#)
- Section of the RFQ
  - [RFQ Section 5.1 - Phase 1 Technical Evaluation platform requirements](#)
  - It states in sub bullet two “Maintaining a reliable, secure bug bounty SaaS platform.
- Question
  - Can the government define the requirements the solution must meet in order to be compliant with the reference of Maintaining a reliable, secure bug bounty SaaS platform”?
- Answer
  - The requirement is to comply with RFQ Section 12 - Addendum - Commercial Contract Clauses, IT Security Procedural Guide 09-48, Security and Privacy Requirements for IT Acquisition Efforts, Low Impact Software as a Service (LiSaaS) – IT Security and Privacy Requirements.

---

## Issue #31

- [GitHub link](#)
  - Section of the RFQ
    - [RFQ Section 5.1 - Phase 1 Technical Evaluation platform requirements](#)
    - The Technical Evaluation Google Form - contains three questions. Each question has a field to provide answers.
  - Question
    - Can the government provide any limitations imposed within this form? I.e. What are the maximum character lengths for submitting documentation on the form for each section?
  - Answer
    - The maximum characters permitted per question is 3000 characters, including spaces and punctuation. The prompt has been updated to reflect this limitation.
- 

## Issue #30

- [GitHub link](#)
- Section of the RFQ
  - [RFQ Section 3.2.4 - Quality Assurance](#)
  - Within the Quality Assurance Surveillance Plan form - Section 2.0 - Standard - it states "The contractor shall perform all work required in a satisfactory manner in accordance with the requirements of the PWS" and further in section 2.3 - Acceptance of Services - it states "Acceptance of services shall be based upon compliance with performance standards described in the PWS".
- Question
  - The 2018 solicitation does not make reference to an existing or award. Can the PWS for the 2018 RFQ be provided?
- Answer
  - Clarification: PWS refers to the requirement section of the RFQ, Section 3.0. An amendment will be issued to update section 3.2.4 Quality Assurance.

---

## Issue #29

- [GitHub link](#)
- Section of the RFQ
  - RFQ Section 3.2.2 - Impact Reports  
<https://github.com/18F/tts-buy-bug-bounty/blob/master/2018-procurement/RFQ.md#322-impact-reports>
  - It states “The contractor shall be responsible for providing timely notification to the CO/COR and the TTS Product Owner when activities or issues outside of the contractor’s control may directly impact the contractor’s performance.”
- Question
  - Can the government specify what the desired time frame is for this notification?
- Answer
  - The government and the awardee will work together during post award to determine an agreed upon timeframe for notification.

---

## Issue #28

- [GitHub link](#)
- Section of the RFQ
  - [RFQ Section 3.2.1 - Vulnerability Reports.](#)
  - It states “The contractor will submit through their security disclosure platform vulnerability reports for those on the TTS application list. These vulnerabilities will be triaged and classified based on the severity of the vulnerability before being submitted to TTS.”
- Question
  - Does the 1 business day requirement require that from the disclosure of vulnerability discovery to the vendor include triage and providing a complete vulnerability report including remediation steps to the vulnerability and submit the entire report TTS?
- Answer



- In accordance with RFQ Section 3.2.1 the vendor must notify TTS of the vulnerability, determine the scope, and assigned to the appropriate team within one (1) day.
- 

## Issue #27

- [GitHub link](#)
  - Section of the RFQ
    - [RFQ Section 3.1 - Key Personnel](#)
    - Point number one it states “The contractor shall provide a Technical Account Manager (TAM) as the primary point of contact for the government’s program office to enable timely problem resolution, reporting in a timely manner, and properly aligning staffing requirements. The contractor will be expected to work with the CO/COR and the TTS Product Owner.”
  - Question
    - Does the technical account manager (TAM) need to have Public Trust, or go through the SF85P process?
  - Answer
    - No, this is not a requirement.
- 

## Issue #26

- [GitHub link](#)
- Section of the RFQ
  - [RFQ Section 3.0 - Requirements on disclosure of researchers](#)
  - Within Bounty Pool Management under sub bullet four it states - “Forward to TTS the vulnerability reports, the names of the researchers, and the award amounts.”
- Question
  - Would the government require the name of the researcher if the vendor provides protection for the researchers and considers this information confidential and provides confidentiality assurances for researchers?
- Answer

- In accordance with RFQ Section 12.0 Addendum - Commercial Contract Clauses, FAR Clauses 52.212-3 Offeror Representations and Certifications -- Commercial Items (Jan 2017), the government will require assurances that the researchers who received the payouts are not from countries forbidden to receive payouts from the government. If a researcher's handle and some other information would be capable of providing the government with these assurances, please outline how and it will be considered.
- 

## Issue #25

- [GitHub link](#)
  - Section of the RFQ
    - [RFQ 3.0 - Requirements](#)
    - Within Bug Bounty pool management - under sub bullet three it states “Once classified and deemed within the scope of the vulnerabilities, the vendor will manage payout to the reporter based on the agreed up bounty reward tiers by the contractor and TTS”.
  - Question
    - Can the vendor/contractor manage the payout directly without TTS when a Firm Fixed Price Model is used?
  - Answer
    - Yes, for undisputed payouts, the vendor can manage the payouts directly under our selected contract type.
- 

## Issue #24

- [GitHub link](#)
- Section of the RFQ
  - [RFQ 3.0 - Requirements](#)
  - It states “The contractor will provide a Software-as-a-Service platform, with a publicly-available website, for researchers to report security vulnerabilities on publicly available government websites in a manner consistent with the TTS vulnerability disclosure policy.”

- Question
    - Does the vendor have to disclose the following information based on the 2017 Solicitation under the technical\_file.yaml under Service\_Platform\_Metrics:
      - The number of security researchers on the SaaS platform?
      - The number of companies using the platform for bug bounty?
      - Average times for triage an initial vulnerability report?
      - Average times for responses of researcher questions and follow ups?
  - Answer
    - The 2017 solicitation does not apply to this requirement. The government is seeking quotations based on the requirements within the 2018 solicitation.
- 

## Issue #23

- [GitHub link](#)
  - Section of the RFQ
    - [RFQ 2.0 - Background](#)
    - Fifth paragraph in this section states “Program management services include services related to promotion of the program, tracking and workflow, and payouts”.
  - Question
    - Does the vendor have to specifically publicly disclose tracking, workflow and payout?
  - Answer
    - As outlined within RFQ Section 3.0 Requirements, the vendor must make the program visible to its community of researchers, and be able to promote its presence on the platform to those researchers. The vendor must support features that allow the government to promote the program by sharing information about payouts and specific vulnerability reports. The vendor is not required to publicly disclose all vulnerability reports, or to disclose all aspects of tracking, workflow, and payouts on the platform.
-

## Issue #22

- [GitHub link](#)
  - Section of the RFQ
    - [RFQ 2.0 - Background](#)
    - Third paragraph in this section states “The larger the community of security researchers in the Bug Bounty SaaS Platform provider’s network, the better the chance TTS has of finding bugs and technical issues within their web applications.”
  - Question
    - Specific to the network of security researchers, can the government confirm they are expecting quality over quantity?
    - Is there an expectation that allowed researchers have been properly vetted for trust and skill prior to being included in any test?
  - Answer
    - TTS is not seeking to vet researchers for trust, skill, or quality prior to being included in any test. As outlined within RFQ Section 3.0, Requirements, TTS seeks a fully public bug bounty that allows for reports to be accepted from any eligible security researcher, where eligibility is defined as meeting the platform and vendor’s requirements to participate within the program. TTS is interested in the quality of the reports it receives, and in the features and service a bug bounty platform may offer that contribute to high report quality.
- 

## Issue #21

- [GitHub link](#)
- Section of the RFQ
  - [RFQ 2.0 - Background](#)
  - Third paragraph in this section there is a statement that states “a contractor provides a Bug Bounty SaaS platform that can achieve the goals of the TTS while providing the best value to the government must be one that is well-established.”
- Question

- What metrics will the government use to define a well established Bug Bounty SaaS platform besides the size of the pool of researchers in the community that would use the platform?
  - Answer
    - TTS intends to make a qualitative determination about whether a vendor is well-established rather than relying primarily on metrics as outlined within RFQ Section 5.0 Evaluation Process.
- 

## Issue #20

- [GitHub link](#)
  - Section of the RFQ
    - [RFQ 7.0 - Type of Contract](#)
    - It states the following “Based on the nature of this requirement, the government intends to award a hybrid Firm-Fixed-Price (FFP) and Firm-Fixed-Price Not-To-Exceed (NTE) contract type. The contract will include a FFP CLIN for access to the platform and triage services. The bounty pool will be NTE, with varying vulnerability levels but with all costs paid directly to the researchers.”
  - Question
    - Can the vendor respond with maintaining and coordinating the Bug Bounty program as a complete Fix Firm Price Model?
    - Would this disqualify the vendor if submitting pricing as a complete Fixed Firm Price model, to include the platform, vulnerability management and triage, vulnerability value management, and vulnerability management for all bug bounty challenges?
  - Answer
    - The type of contract will remain as a hybrid Firm-Fixed-Price (FFP) and Firm-Fixed-Price Not-To-Exceed (NTE). All responses must be in accordance with the selected contract type.
- 

## Issue #18

- [GitHub link](#)

- Section of the RFQ
    - [RFQ 5.1 - Phase 1 Technical Evaluation](#)
  - Question
    - Is there a response length limit for the technical evaluation?
  - Answer
    - Please see Issue #31 response.
- 

## Issue #17

- [GitHub link](#)
  - Section of the RFQ
    - [RFQ Addendum - Commercial Clauses, Low Impact Software as a Service \(LiSaaS\) – IT Security and Privacy Requirements](#)
  - Question
    - Even though security vulnerability data is in-scope, only FedRAMP Tailored LI-SaaS or FedRAMP Low is required in order to meet the FedRAMP compliance requirement (within 1-year after contract date), correct? Just want to make sure we understand the impact level required for this project, as per FIPS PUB 199.
  - Answer
    - A GSA LISaaS 1-year ATO is required to begin use of the product, and should be completed expeditiously upon award. Within 1 year of contract date, a FedRAMP Tailored or Low authorization is required in order to continue using the product. GSA would authorize the system at a Low impact level as per FIPS PUB 199. Though the system stores security vulnerability information, researchers are not given credentialed access, and so all vulnerabilities are publicly discoverable. TTS considers these reports already publicly known or knowable, and quickly resolves any significant vulnerabilities.
- 

## Issue #16

- [GitHub link](#)
- Section of the RFQ

- [RFQ Addendum - Commercial Clauses, Low Impact Software as a Service \(LiSaaS\) – IT Security and Privacy Requirements](#)
  - Question
    - Is it expected that we use an external 3PAO for FedRAMP assessment, or would the GSA be our independent assessor?
  - Answer
    - GSA will facilitate the initial LiSaaS assessment for a 1 year ATO. Offerors will be required to work with GSA and submit requested documentation expeditiously to achieve the initial 1 year ATO. FedRAMP Tailored assessment of the implemented controls may be performed by an independent trusted third-party, a FedRAMP Accredited Third-Party Assessment Organization (3PAO) at the vendor's option and cost.
-