EFiling Check-In - Oct 07, 2021

# Attendees:

* Wei Luo
* Ken Lally
* Laura Beaufort
* Ryan Lanz
* Jonella Culmer
* Robert Fultz
* Alex Lin
* Matt Travers
* Al Crowley

# Discussion Notes:

* These notes capture discussion points and action items not covered in materials provided.
  + Slide Deck: “FEC - FECFile Online - Weekly Check-in - 2021-10-0.pptx” for slide deck content
  + QASP matrix with proposed tools: Quality Assurance Surveillance Plan - Form 3X Bundle Assessment - 2021\_10\_07.xlsx
  + Response to Questions from FEC.docx
* Schedule (p4):
  + Regarding OWASP ZAP risk, Laura clarified that FEC is open to utilizing comparable tools if OWASP ZAP proves challenging to stand-up in this timeframe.
  + For review of automated tool outputs, TCG will coordinate with FEC per output, given that different FEC staff will have different expertise.
  + Jonella asked a question about what the length of the reporting period is.
    - Alex responded that we have assumed a weekly cadence for the check-ins.
    - The group agreed that, for now, this was sufficient.
* Staffing and Resources (p5):
  + Jonella clarified that both she and Robert can be a resource to the team for questions on 508.
  + *Note:* After the meeting, Ken Lally provided clarifications around the role of Product Owner, which have been updated in the slide deck.
  + **Action Item:** Alex to coordinate with Ryan Lanz for demos of the three systems
    - Jonella asked that she and Robert be included in the demo
    - Ryan will review the Dev, QA, and UAT environments to ensure that he still has access to them.
  + **Action Item:** Alex to reach out to Paul Clark for access to the Jira board provided in FEC’s responses.
  + **Action Item:** Slack was agreed on as the preferred platform for collaboration. Alex to coordinate with FEC to get Slack capabilities tested.
  + On the question of a private repository for the TCG team’s work in the fecgov github space:
    - Laura expressed a preference to include all materials in the public space to support FEC’s philosophy of working in the open
    - Ryan expressed some concerns about keeping all materials in the public space--for instance, meeting notes for certain meetings might need to be kept in a private repository.
    - Alex offered that a follow-up conversation is probably needed to establish a rubric for what is public vs. private.
    - **Action Item:** Alex to start and coordinate a follow-up discussion around the public vs. private repository.
* Risks and Issues (p7):
  + Ryan noted that one risk to the FEC is that the required date for exercising the option period is coming up quickly (i.e. because of the requirement of 30 days notice to exercise the option) and there is not currently a deliverable scheduled before then.
    - Wei responded that there have been some discussions with the CFO on this topic.
    - Alex offered that TCG is willing to work with FEC to define a deliverable or other evaluation criteria to support FEC’s decision making.
    - **Action Item:** Alex to follow-up with FEC on potential needs for an interim deliverable to allow for fair evaluation.
* Debrief:
  + Alex asked if the provided slide template was a reasonable format for the weekly check-ins.
  + Jonella responded that the format seemed fine for now and that we could adjust later if needed.
    - The rest of the group concurred.
* Follow-up Discussion of Answers Provided by FEC:
  + P1: From FEC, in response to the question about prioritization of 18F’s 4 recommendations: “...Could you explain in more detail your concern regarding this question?”
    - Alex clarified that this was a probing question intent on gauging how wholeheartedly 18F’s recommendations have been adopted--at other agencies, TCG has seen that the recommendations of third party assessments receive mixed assessments and prioritization. The answer provided makes clear that the recommendations have a high level of support from FEC.
  + P2: FEC asked for clarification around the instance of fecfile-validate running in the cloud.
    - Alex explained that this instance of fecfile-validate is explicitly mentioned in the jenkins scripts, and that the TCG team was wondering if it might be a development instance.
    - Ryan clarified that this instance does not seem to be one of the official Dev, QA, or UAT instances. He will provide access to those if possible.
* QASP Tools Review:
  + The goal of this review was to confirm some of the automated tools selected for the first part of the assessment (i.e. assessment of existing code against the Quality Assurance Surveillance Plan)
    - Methods/tools listed were confirmed by FEC, with discussion as noted below.
  + On code style, Laura noted that FEC would be willing to review recommendations from TCG about what constitutes actionable findings from the linting tools.
    - **Action Item:** As part of review of the automated tools, TCG will provide recommendations and narrative about what we believe is actionable (i.e. vs. false positives).
  + On 508:
    - HTML Code Sniffer was accepted as a substitute for the listed 508 tools.
      * Laura noted that the amount of manual intervention needed for HTML Code Sniffer, while acceptable for the assessment, would not be an accepted solution for future development work, as it cannot be automated as part of a CI/CD pipeline.
  + On security:
    - The TCG team asked if Sonarqube could be substituted for bandit (Sonarqube is a standard TCG tool and--in some respects--more robust.)
      * Laura responded that FEC would be willing to accept the substitution if a side-by-side comparison demonstrates that Sonarqube covers all bandit findings.
        + Matt confirmed that this would be possible.
      * Laura reiterated that FEC would accept a substitution for OWASP ZAP if necessary.