Evolving the CDE: Discovery

Status Report (11/13)

18F

Project plan

Timeline: We are here (11/13) — THANKSGIVING (11/20) — HOLIDAYS (12/25)

Dates: 10/30, 11/6, 11/13, 11/20, 12/4, 12/11, 12/18, 12/25, 1/1, 1/8, 1/15, 1/22

PLANNING & KICKOFF | **PROTOTYPING** (SPRINT 1, SPRINT 2, SPRINT 3, SPRINT 4) | **SYNTHESIS**

PRIORITIZE FOCAL AREAS | SPRINT-BASED OUTPUTS (REFERENCE DESIGN, PROTOTYPES, KEY INSIGHTS, TECHNICAL FINDINGS, USER STORIES) | DOCUMENT KEY FINDINGS
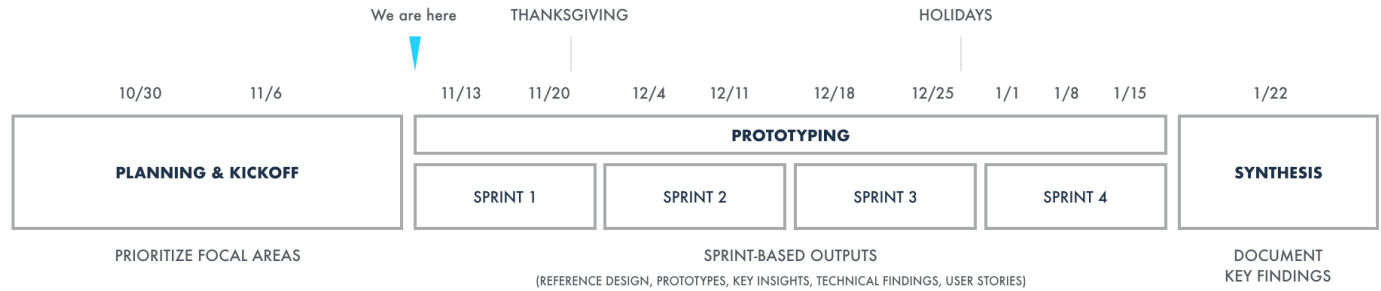
Executive Summary of Activities:

Last week 18F focused on synthesizing what was learned from the project kickoff on 11/2 and preparing for the first discovery sprint. During the kickoff we identified several "opportunity areas" for improving the CDE. Since the purpose of this discovery effort is to inform the future of the product by understanding what is important to build and why, we asked the participants from the kickoff to rank these opportunities by perceived value and uncertainty. "Expanding the volume of NIBRS data available" was the highest ranking opportunity area.

With this general direction established the team has scheduled a working session with Cindy, the CDE Product Owner, to define criteria (e.g., problem statements and assumptions to test) that will guide the first round of discovery activities. 18F may use a variety of techniques, ranging from general research to prototyping, to answer the questions prioritized by Cindy and so the exact nature of our activities will depend on the problem set selected. At the conclusion of each sprint we'll share the key lessons learned and use them to inform the next round of testing.

In addition to planning for sprint 1 the team has been working with Jacob Wentz at CJIS on a few NIBRS-related data quality issues, specifically an issue where we misrepresent the number of offenders & victims related to an incident with multiple offenses recorded. We think we understand the problem and are working on a solution. We've also been coordinating with Jacob on an odd dip in NIBRS participation for 2015. After some investigation by Jacob it seems that a few tables related to the 2015 import will need to be regenerated in order to fix this problem. You can view what else the team is working on here: https://waffle.io/18F/crime-data-explorer.

Finally, as part of its planning activities last week 18F developed a memo on how quantitative data provided by platforms like the Digital Analytics Program (DAP) could be used to evaluate the performance of the CDE and inform decision making around the product. 18F recommends that CJIS takes this opportunity to define clear success criteria for the CDE and identify relevant metrics that help measure progress towards those goals.

Open Issues:

- Currently on production we are [missing a glossary definition for the term "reported"](#) in the agency view legend. This is due to an earlier change where we originally changed the legend from "reported" to "actual" to more accurately reflect the fields where the data was being pulled from. However, the use of "actual" was problematic because the CDE shows reported crime; it doesn't reflect the outcomes of the criminal justice system. Moving forward we should develop a new definition to be displayed for "reported." Jeremia has suggested: ***"The number of offenses reported to and known by law enforcement that are not subsequently determined to be unfounded."***
- We need to define an approach that promotes visibility across the various work streams supporting the CDE. 18F is tracking its discovery work in Waffle and CJIS is tracking new feature development. Since discovery will feed development it is important that both teams have visibility into what is being worked on.
- The Cloud.gov team has completed its "research spike" around the possibility of implementing DNSSEC for Cloud.gov. Currently Cloud.gov does not support DNSSEC, although its mitigations has been approved by the Joint Authorization Board (JAB), and this has been cited as a blocker to obtaining an FBI.gov URL for the CDE. After conducting its research the Cloud.gov team has agreed to implement DNSSEC; however, the earliest it can start working on it is early January due to current priorities and then the change will need to be approved by the FedRAMP JAB, which could take an undetermined amount of time.