Project Boise

Phase 3 Proposal

18F Aidan Feldman, Andrew Maier, Tim Jones

Overview

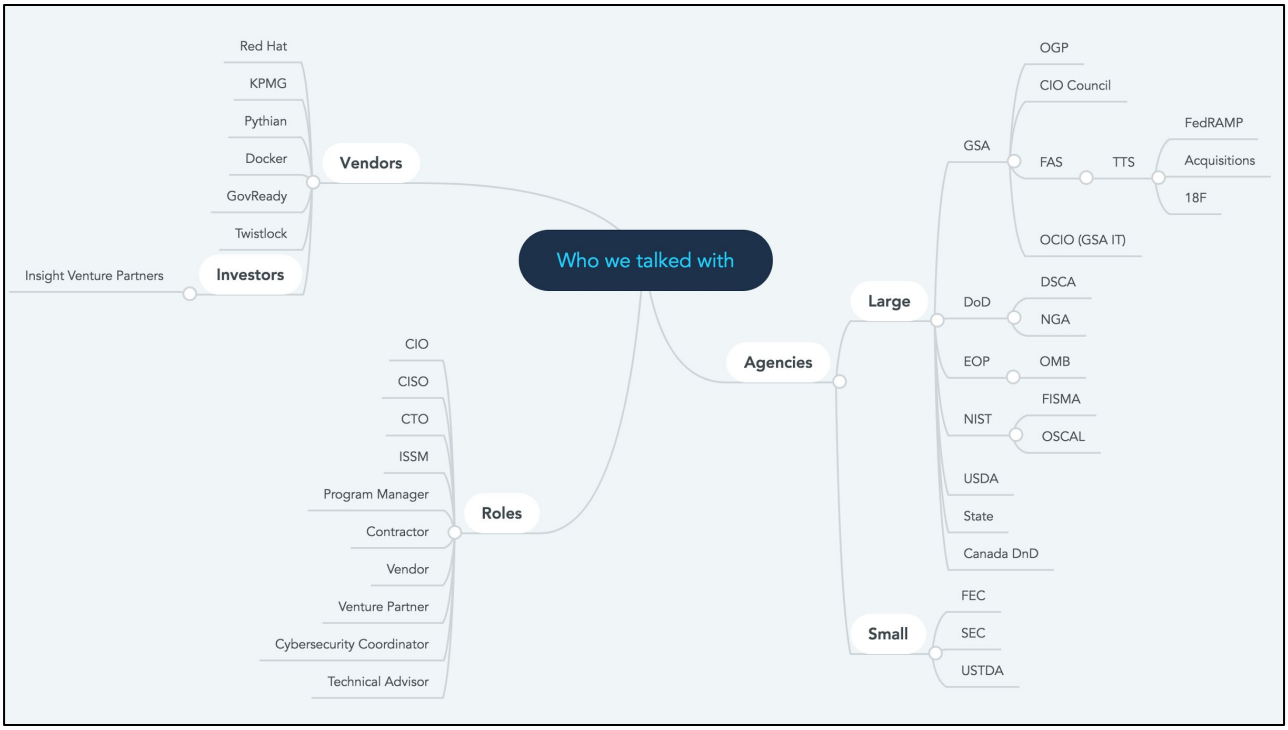
1. What is Project Boise
2. What we did
3. What we learned
4. What’s next

Project Boise aims to reduce the burden and improve the effectiveness of the federal government's software security compliance processes.

(time, cost, and pain)

2/ What we did

What did we do?



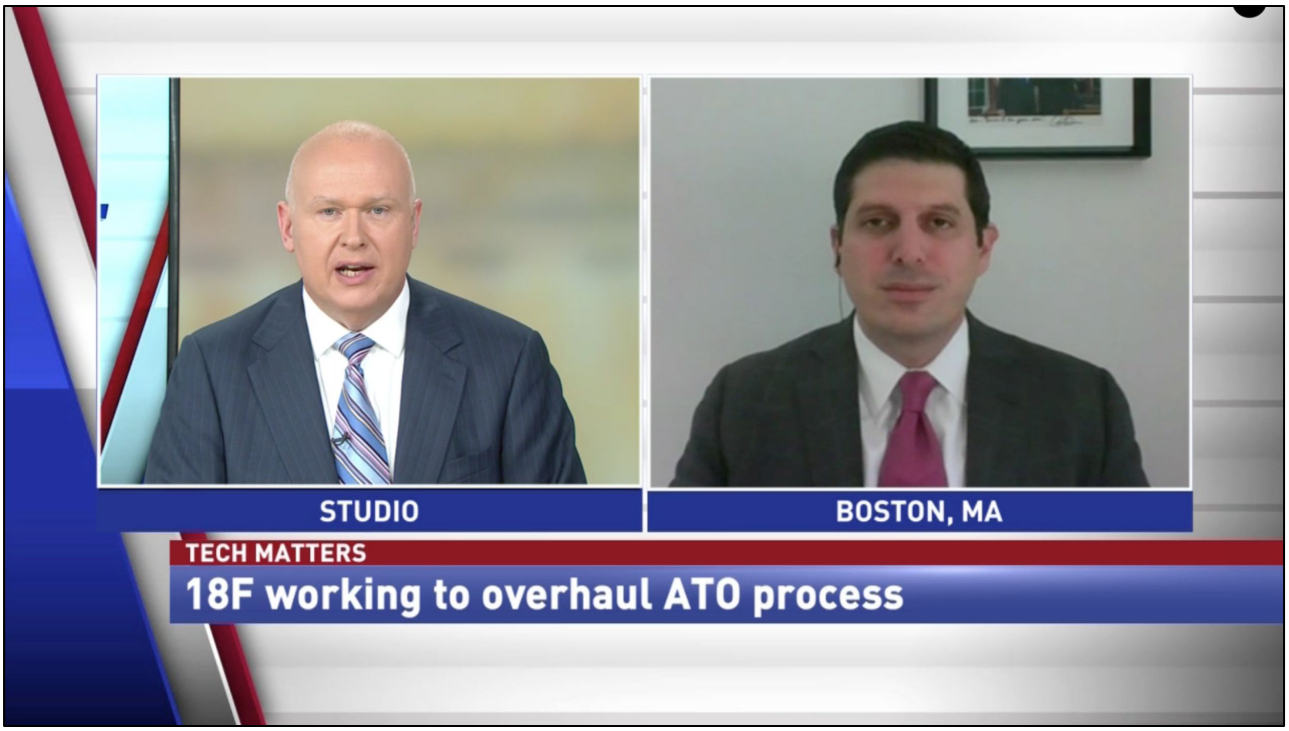
- We talked to people
- 25+ interviews with 30+ stakeholders
- Tried to cover a broad range of perspectives
- The more people we talked to, the more people we realized we *could* talk to

https://www.mindmeister.com/953123419

3/ What we learned

There was a surprising amount of interest in Project Boise

- Several articles
- A well-circulated blog post by Nick Sinai, the former US Deputy CTO
- Invited to be on multiple panels
- We even got…



- …a segment on ABC News
- Given the attention, people eagerly reached out, because they heard we were here to “fix” ATOs
- We had to turn interviewees away
- We believe we got all this attention because...

http://govmatters.tv/18f-working-to-overhaul-ato-process/

Compliance sucks, for everyone involved

- Even the people who write the rules are frustrated that they are being misinterpreted in a maximalist way

Compliance creates a culture of fear

- It's referred to as "risk management", but most of the risk that's managed is from internal oversight, not external threats like hackers.
- No one wants to show their dirty laundry
- Culture of secrecy
- Groups can't learn from one another, meaning they don't build off one another or collaborate

Compliance Masonry is our dark horse

- So what is Compliance Masonry?
- A tool to manage, combine, and transform security control content
- In other words, a package manager for compliance documentation
- Cloud.gov has been developing it initially, but it was sidelined for practical reasons
- Compliance Masonry has experienced substantial organic growth
- In use at multiple agencies and companies already
- Multiple products are being built around it
- Included in Red Hat Enterprise Linux by default...

3+ million installations (!!!)

- ...installed on 3-4 million machines
- Why is this important?
  - It can cut down the time to initial ATO substantially
  - Reduce time explaining how a system is secure, so time can be spent making the system secure
- What's it missing?
  - Number one question and barrier to adoption we hear is "does it have GSA support?"

4/ What’s next

Phase 3:
Double down on Compliance Masonry

- In Phases 1 and 2, we worked to understand the space
  - Feel we've gained a good grasp
- Given what've learned, we want use Phase 3 to narrow focus to improving the path to initial ATO
  - Compliance Masonry
    - Improve its onboarding experience and documentation
    - Make it easier to understand and use
  - We're already identified promising partners from our Discovery
    - Work with vendors to produce Compliance Masonry-consumable content, which will only improve the value-add
- Compliance Masonry is something small that works, and that we want to make work better
- We have Compliance Masonry, a central tool we can use to get in the door
  - Like US Web Design Standards
- With the tooling, we want to provide guidance and reform

The long game:

~~Project Boise~~

TTS Compliance Engineering

18F

- Our long game is a TTS Compliance Engineering team
- After Phase 3, we want to expand our offerings and work to improve additional areas of the risk management process, from various angles
- This is where Project Boise goes from being a product to a program
- Like TTS Acquisition does for procurement, we want to do for compliance

We aren’t proposing a solution.
We’re proposing a learning mindset.

- There is no silver bullet
- Questioning the compliance process isn’t built into the compliance process, much less improving it
- We hope to change that
- We believe that the benefits of knowledge and materials sharing, as well as collaboration around software security outweigh those of secrecy
- We believe bringing design thinking and focus on efficiency and effectiveness to compliance can change the game, and that TTS is the team to do it
-

Thanks!

#project-boise

boise.18f.gov

18F