SAN FRANCISCO DEPARTMENT OF TECHNOLOGY

Date: March 17, 2019

To: John Arntz

From: Linda Gerull

Subject: Open Source Voting Project Status – March 2019

The status and next actions for the Open Source Voting Project are the following:

1. The Open Source Voting Project is moving forward in the Planning and Discovery phase.
    - An opportunity to discuss a current Open Source project for elections was discovered. The Project Sponsors reviewed the strategy and direction of this Project as well as met with the technical managers.
    - A Washington Post press release (attached) described how DARPA will be re-engineering voting machine hardware to be secure from cyberattacks.
    - Next action: Consider how current Open Source Projects and future DARPA hardware could be of use to the City's efforts.

2. The Open Source Voting Project is moving forward in the Requirements Definition phase.
    - Requirements for the system are being defined.
    - Next action: review with the Technical Advisory Board.

3. The Open Source Voting Project is taking steps to begin the Community Engagement phase.
    - The Community Engagement meeting is scheduled for April 26 at 3:00.
    - Next action: Develop an agenda for the Community Meeting with OnStrategy.
    - Next action: Work with TAC to develop a contact list for announcing the community engagement meeting.

4. The Open Source Voting Project continues to add resources to deliver the project.
    - The OSV Sponsors are reviewing the proposals from the Request for Proposal for Professional Services to assist with the development of project deliverables.
    - Next action: Select a vendor to complete project deliverables.

Washington Post

DARPA has a plan to making voting machines far more secure

By Joseph Marks

The Pentagon research agency that played a key role in inventing GPS and the Internet has a plan to make voting machines far more secure against hackers.

The Defense Advanced Research Projects Agency intends to re-engineer voting machines' hardware – basically the machines' physical components, such as computer chips and circuits – so that many of the tricks hackers use to undermine the software become impossible.

That's a fundamentally different approach from most cybersecurity efforts, which focus on updating and patching software each time a new bug is discovered.

If the project is successful it will make it far more difficult for hackers to penetrate and manipulate voting systems as Russian hackers tried to do in 2016. There's no evidence Russian hackers actually penetrated machines, but the effort — along with a broader hacking and disinformation campaign targeting Democratic nominee Hillary Clinton — sparked big questions about the influence of foreign actors in U.S. elections and ultimately led to a probe of possible ties to the Trump campaign by special prosecutor Robert Mueller.

"This seems to us to have a deep national interest," Linton Salmon, the DARPA program manager leading the project, told me. "Most of us want to make sure our votes get counted."

One big hurdle: There's no requirement for voting machine vendors that supply states with election equipment to adopt the new hardware. Once DARPA achieves its goal, it plans to simply publish all the technical details so any organization that wants to build the new machines can do so.

There will likely be intense pressure on election vendors, however, to adopt the hardware from the election security community, which has criticized vendors for being opaque when it comes to protecting their machines.

The project is part of a broader DARPA effort to use more secure hardware to protect against hacking in numerous sectors -- including at energy plants, financial services firms and the defense industrial base. By making voting machines their first focus area, the agency hopes to excite the interest of the tech industry and the broader public and to help boost security in a highly important area, Salmon told me.

“The intention…is not just to protect DOD systems. It’s to protect everybody,” Salmon said.

The project won't be complete for another two years, however, and it often takes a year or more to replace a digital system's hardware. So it's unlikely to achieve its goal before the 2020 elections.

DARPA has awarded about $15.5 million to eight grant recipients to work on the broader hardware project. It awarded another $4.5 million to the Portland, Ore., security firm Galois to apply those hardware fixes to real-world threat situations – in this case, voting machines.

Galois unveiled the voting machines at a George Washington University election security conference Thursday. DARPA and Galois plan to take their prototype voting machines to the Def Con hacking conference in Las Vegas in August where they’ll invite ethical hackers to try to crack into them. Hackers at that conference found numerous vulnerabilities in existing voting machines during last year’s conference.

After Def Con, DARPA and Galois want to take the machines on a tour of universities where they’ll do similar live-fire testing with graduate computer science students. Then they’ll bring an improved system back to Def Con in 2020.

“We feel the best way is to open it up to the best hacker community in the world,” Salmon told me. “This is getting us a lot better evaluation than we’d get from hiring five gurus to attack it.”

The revamped hardware won’t protect against all potential software hacks, Salmon warned — just against seven main categories DARPA believes can be fully thwarted with a hardware rewrite and that accounted for about 60 percent of all known software vulnerabilities as of 2015.

There are other categories of hacks, though, that don’t have a hardware fix, so the new system wouldn’t be a replacement for other election-security efforts, such as mandating paper ballots or auditing election results.

During the same conference where Galois unveiled the voting machine program, Sen. Ron Wyden (D-Ore.) accused voting machine makers of refusing to answer questions about their security and valuing profits over the integrity of votes.

“The maintenance of Americans’ constitutional rights should not depend on the good graces and sketchy ethics of a handful of well-connected corporations,” Wyden said.

Timed with the conference, Wyden reintroduced an election security bill, the Protecting American Votes and Elections Act, which would authorize the Homeland Security Department to set minimum cybersecurity standards for voting machine makers.