FOR IMMEDIATE RELEASE AUGUST 12, 2018
Contact: Molly Hall, 202-210-9955 or mhall@cambridgeglobal.com

Voting Village at DEF CON Promotes Election Security and Integrity

Las Vegas, NV - The Vote Hacking Village ("Voting Village") had an exciting three days at DEF CON 26, the largest hacking conference in the world. DEF CON brings together a wide range of hackers, corporate IT professionals, policymakers, and others interested in computer security and related issues. The Voting Village, now in its second year, addresses election security issues and invites attendees to study and identify vulnerabilities in election equipment used around the United States as well as other nations.

The Voting Village was ecstatic to have a senior leader at the NSA and former Trump White House Cyber Czar, Rob Joyce, in attendance, who lauded our efforts, saying that "Believe me, there are people who are going to attempt to find flaws in those [election] machines whether we do it here publicly or not. So, I think it's much more important that we get out, look at those things, and pull on it." Joining Mr. Joyce in the Voting Village over the course of three days were thousands of hackers, over 100 election officials, and about 50 kids identifying and exploiting various vulnerabilities within the election ecosystem.

The Voting Village has dramatically expanded this year to include not only more machines but also end-to-end voting infrastructure including a voter registration database and election reporting websites. This year's Voting Village featured hands-on experience with at least nine types of voting equipment (voting machines, e-poll book system, and election-related security appliances) almost all of which are in use in elections today. In addition to the machines, the Voting Village featured a (greatly improved from last year) cyber range that allowed election officials to be trained in defending a voter registration database from hackers and simulated state-of-the-art attacks.

The Voting Village had participants find or replicate vulnerabilities ranging from passwords stored on the machines with no encryption to buffer overflows in critical input routines. Specific hacks included:

- Hacking a voting machine to play gifs and music;
- Discovering 1784 files, including mp3s of Chinese pop songs, hidden among the operating system files of another voting machine;
- Hacking a mock election so that an un-listed candidate received the most votes;
- Hacking an email ballot so that the recorded vote was different from what was selected; and
- An 11-year-old hacking a replica Secretary of State website within 10 minutes.

The Voting Village will release detailed findings at a later date after close analysis and appropriate process.

By allowing DEF CON participants to examine election equipment and report on the results, the Voting Village has raised public awareness about election technologies and seeks to encourage election equipment vendors to improve the security of their systems. Matt Blaze, co-founder of the Voting Village said, "It's been incredible

the response we've received. We've had over 100 election officials come through here and they expressed over and over again how much they have appreciated learning from this opportunity." Another Voting Village co-founder, Harri Hursti, expanded on that saying, "the election officials and senior federal cyber professionals have reiterated that they cannot defend against the unknown. They can only mitigate against vulnerabilities they know about."

Although the weekend was a huge success for our elections, one election machine manufacturer—Election Systems and Software ("ES&S")—has taken the opportunity to raise some questions about the value of the Voting Village. It is unfortunate that ES&S is making vague and unsupportable threats that distract from the real issue: the integrity and security of our electoral process. In light of ES&S's statements, the Voting Village retained Protect Democracy and Harvard Law School's Cyberlaw Clinic to advise us on our legal position.

We at the Voting Village, along with our counsel, remain confident that our activities are lawful and are happy to address any of ES&S's legal concerns directly. ES&S's unclear comments and threats towards the Voting Village seem to be designed to create questions and cast doubt in the minds of researchers and election officials, discouraging them from pursuing these vital lines of inquiry. At a time when there is significant concern about the integrity of our election system, the public needs now more than ever to know that election equipment has been rigorously evaluated and that vulnerabilities are not just being swept under the rug.

The Voting Village is eager to work with ES&S and other manufacturers next year and we invite them to collaborate with us and attend DEF CON 27 in 2019, just as we have previously. When the security and integrity of our elections are at stake, the Voting Village will continue pushing forward in its mission to ensure that any vulnerabilities within our election ecosystem are identified and rectified. We will detail the various vulnerabilities in a comprehensive report and will continue to advocate on this important issue.

The Voting Village is co-founded by Jake Braun, Matt Blaze, and Harri Hursti. Jake Braun is Chief Executive Officer of Cambridge Global Advisors, Executive Director of the Cyber Policy Initiative at the University of Chicago, and has over fifteen years of experience in the development and implementation of strategic direction for complex, high profile national security initiatives (including as White House liaison for the Department of Homeland Security in the Obama Administration). Matt Blaze is a Professor of Computer and Information Science at the University of Pennsylvania, where he researches secure systems, cryptography, and trust management. Harri Hursti is the founder of Nordic Innovation Labs and is a world-renowned expert on data security, with a particular focus on elections. He received the Electronic Frontier Foundation Pioneer Award in 2009 for his work in election security.
