Election Process Protection: Location Specific Custom Study, Registration, Voting Tallying, and Recommendations

LEXINGTON, Massachusetts (June 8, 2017) – WinterGreen Research announces that it has published a new study Voting Center Vulnerability: Market Shares, Strategy, and Forecasts, Worldwide, 2017 to 2023. Political campaigning accounting for billions of dollars in spending, and domination of the news cycle (as James Michael Curley said so famously, "Just spell my name right") get all the headlines. But what really matters in the end for the democratic process is the mechanics of running the election. We need a process that cannot be subverted. Countries, nations, states, regions, and counties need a process that counts the votes accurately and lets all qualified people vote.

Democracies need a vote counting process that makes all fraud detectable immediately as the votes are being counted, there needs to be protections built in so that all observers, including the independent media have instant confidence in the integrity of the election process.

The WinterGreen Research study is customized for each client. The breadth and depth of the laws, systems, and procedures used, the variety of voting registration systems and vote counting systems make it impossible to cover all those in depth in one study. The study gets too long. Instead this customer study is written in two weeks in response to input from a survey that collects information about the particular system being used.

Russian efforts to hack voting systems in the United States have been well publicized. What has been less apparent is the inherent vulnerabilities of many of the voting systems in the US and elsewhere.

Prelude to Custom Election Process Research: James B. Comey, former director of the F.B.I. Has indicated that Russian operatives intervened in the 2016 presidential election and that it could happen again. Russian hackers are the best in the world, that is why they are so good at building computer security systems, because they know how to hacek.

Russian hackers breached Democratic email accounts; they orchestrated a hack that targeted thousands of US government state and local databases.

Apparently Russian computer hacks harvested emails from the State Department and the White House. They apparently penetrated deep into the computer systems of the Joint Chiefs of Staff.

The Russian effort to manipulate American politics is serious and needs to be addressed by the people responsible for running elections in the US.

Graham Allison, a longtime Russia scholar at Harvard, said, "Russia's cyber intrusion into the recent presidential election signals the beginning of what is almost sure to be an intensified cyberwar in which both they -- and we -- seek to participate in picking the leaders of an adversary."

The difference, he added, is that American elections are generally fair, so "we are much more vulnerable to such manipulation than is Russia," where results are often preordained...

In the intelligence community, James R. Clapper Jr., has sounded the alarm since retiring in January. He was director of national intelligence. "I don't think people have their head around the scope of what the Russians are doing," he said recently.

Russia is coming after us, but not just the U.S., but the free world in general. In order to take this threat to our national existence, election officials need to take this seriously.

Each locality, be it a country, a state, a region, a city or county has different election systems that are responsive to the local conditions. This is as it should be. Elections are inherently local. The best protections for accuracy and reliability of the voting systems come from local involvement in the process, in the registration process and the vote counting process. The local people are the best independent observers.

The security of the systems needs to be reflective of the inherent transparency that is achieved when watchers from opposing parties are able to watch the process in depth. No part of the process should be secret. When the author of this study, as a consultant, worked set up the State Board of Elections in Illinois, the most effective systems initiated were those that made the process transparent to representatives of both parties. The JFK Kennedy election had been stolen and JFK himself was appalled by the illegality of the election and put in process ways to correct the election process to prevent the stealing elections.

More needs to be done now. More can be done than has been done to prevent Russian efforts to hack voting systems in the United States and other places. This study represents a step, a guidepost if you will, to preventing hacking and to setting up systems that are secure.

According to Susan Eustis, lead author of the team that prepares the study, "Growing accountability of the election process needs to happen to protect a democracy. Election computer systems present great vulnerability and need to be designed in a manner that protects the integrity of the vote registration and the voting counting process. Administrators are realizing the benefits as related to the quality of high quality, low cost systems."

The complete report is a customized look at provides a comprehensive analysis of Elections Systems Practice Computer Security threats in different categories, illustrating the diversity of election vulnerability in the software market segments. A complete procedure analysis is done, looking at procedures and penetration analysis.

Data is collected from the headquarters of the National Security Agency and from state capitals that have discovered that the Russians were inside their voter-registration systems. An analysis is further provided to get people and election officials to look more deeply into the vulnerabilities of the vote tallying systems.

We now know Russia disrupted American democracy in 2016 and there is an effort to provide practical advice on how to prevent fraudulent behavior from influencing the outcome of an election. The recommendations help prevent this type of computer fraud from happening again. Russian hackers did not just breach Democratic email accounts; according to Mr. Comey, they orchestrated a "massive effort" targeting hundreds of, and more than 1,000 of, American government and private organizations since 2015.

WinterGreen Research, Inc.
6 Raymond St.
Lexington, MA 02421
(781) 863-5078   info@wintergreenresearch.com
www.wintergreenresearch.com

WinterGreen Research is an independent research organization funded by the sale of market research studies all over the world and by the implementation of ROI models that are used to calculate the total cost of ownership of equipment, services, and software. The company has 35 distributors worldwide, including Global Information Info Shop, Market Research.com, Research and Markets, electronics.ca, and Thompson Financial. It conducts its business with integrity.

The increasingly global nature of science, technology and engineering is a reflection of the implementation of the globally integrated enterprise. Customers trust wintergreen research to work alongside them to ensure the success of the participation in a particular market segment.

WinterGreen Research supports various market segment programs; provides trusted technical services to the marketing departments. It carries out accurate market share and forecast analysis services for a range of commercial and government customers globally. These are all vital market research support solutions requiring trust and integrity.

Contact:

Susan Eustis, President and Co-Author   (781) 863-5078 (Work)
WinterGreen Research   (617) 852-7876 (Cell)
6 Raymond St.   susan@wintergreenresearch.com
Lexington, MA 02421   www.wintergreenresearch.com

Key Words:. Computerized Registration Systems, Computer Tallying, Protection of the Democratic Process, Large Group Voter Registration Systems, Rules Based Election Coding Technology, Vote System

Coding, Democratic Protections Necessity , Voting Systems Records, Electronic Vote Coding , Protections for Vote Systems Solutions, Computerized Voting System Workflow , Claims Adherence, Terminology Supported Candidate Management, Electronic Coding for Election Officials, Election Protection Necessity, Correct Coding Tools, Electronic Election Record Systems, Language and Computing, Recommendations for Security Protection of Solutions, Diagnosis of Security Vulnerability, Procedure Coding, Registration Systems Natural Language Coding , NLC, Computer Assisted Coding , CAC, Voting Systems Standards