# Evansville Courier and Press

# Editorial: Integrity at the ballot box

Evansville 7:28 a.m. CDT September 29, 2016

One of the last questions asked of Hillary Clinton and Donald Trump at their first debate at Hofstra University deserves to be revisited. Moderator Lester Holt asked both candidates whether, if they lost the election, they accept the results as the “will of the voters.” Both indicated that yes, they would (although Trump agreed to support Clinton so reluctantly — it required a follow-up question from Holt — that reporters felt compelled to confirm his position afterward).

In any other presidential race, a question about recognizing the will of the voters would be regarded as a softball — the answer so obvious that surely no debate prep was needed. After all, what kind of presidential nominee seeks to delegitimize the essential process that sustains the greatest democracy on earth? But these are not ordinary times.

The nation’s voting system faces a very real threat from computer hackers. That much was made clear with the breach of a voter information database in Illinois this summer. Election boards across the country were put on alert by federal authorities out of concern for potential vulnerabilities.

Such a problem deserves to be taken seriously, yet the biggest threat of all may be one not so easily addressed in the final six weeks of the campaign: What if the public loses confidence in the voting system and judges it so unreliable that voters do not believe the winner of the election is necessarily the winner at all?

Experts in cyber security worry that this sowing of doubt within the electorate is far more worrisome than anything a hacker could achieve. After all, there are significant protections already in place — from disconnecting voting machines from the internet to educating election officials on how to spot a potential breach of the registration or absentee ballot databases. According to a recent report by the Brennan Center for Justice, about 80 percent of votes cast on Nov. 8 will leave behind a “paper trail,” meaning they can be double-checked without use of any electronic technology.

Some of these security enhancements stem from the last truly close presidential election, the 2000 contest between Al Gore and George W. Bush that came down to a dispute over Florida and its “hanging chads.” The subsequent reforms include the use of ballot scanner systems that maintain a paper trail, federal certification of equipment and a disconnect from the internet (even now, the overwhelming majority of voting isn’t online).

Yet there are also added vulnerabilities: The election may be close, and the issue of cyber security is sensationalized given that Republicans for years have been attacking the integrity of the U.S. voting system with red herring claims about the need for photo identification cards — supposedly to counter in-person ballot fraud, which is virtually non-existent, but actually in order to quash turnout by minorities and others who tend to vote Democratic. It’s also unhelpful that Trump’s anti-establishment campaign has been stoking fears of a “stolen” election for months. Some days, it’s going to be stolen by party leaders rigging the nominating process, and more recently the finger of blame has landed on the lack of ID laws (leading Trump to ask his supporters to volunteer as an army of poll watchers in places like Philadelphia with its large African-American vote).

In testimony heard Tuesday by the House subcommittee that oversees information technology, it was clear that there’s much more the nation needs to do to protect election integrity — particularly by focusing on real problems like replacing outdated equipment that might be manipulated remotely (in the 14 states that went paperless, for example) and not on greatly overstated problems like people showing up at the polls claiming to be someone they are not. Here’s the real nightmare scenario: What if there is evidence of hacking in a swing state where there is no paper trail? Or what happens if thousands of people in those states have been wrongly purged from the voting rolls and can’t cast a ballot at all? What if all that hacking is traced to foreign agents? Again, that’s worrisome, but it’s exactly what authorities are now working to prevent.

In the long term, there are numerous reforms needed, from replacing old machines to ending the practice of voting over the internet. In the near-term, election boards must do all they can to recognize and address existing vulnerabilities — including auditing the final results. Still, it would be wise for the candidates and their supporters not to overstate or sensationalize the problem and certainly not to goad supporters into rejecting the outcome before it’s even known. Trump and Clinton set a reasonable standard at the debate when the issue was raised. Now they need to stick to that standard and not casually raise undue alarm over the integrity of what remains — at least until proven otherwise — a respectable election process.

*This editorial first appeared in the Baltimore Sun.*