DALLAS COUNTY ELECTIONS DEPARTMENT

October 2, 2017

FOR IMMEDIATE RELEASE: PRESS RELEASE

From: Toni Pippins-Poole, Elections Administrator, CERA, CCPA

Dallas County Elections Administrator Responds to Reports of Cyber-Security Threats Related to Voting

Recently, comments were written by the media questioning whether Dallas County Elections Department's (DCED) information and equipment resources were hacked by Russian infiltrators during the November 2016 Presidential Election. This press release is meant to clarify the statements of DCED's Elections Administrator, Toni Pippins-Poole (Pippins-Poole), and to ensure the public regarding Dallas County's resolve in protecting election and voting equipment, processes, data and information resources.

Please note that much of the information related to this discussion was provided and accepted on a "DIRECT NEED TO KNOW BASIS", and therefore cannot and should not be divulged beyond a certain point.

In June through November of 2016, Dallas County participated in and cooperated with Federal organizations to review, prepare for, test and safeguard election and voter related information systems from very real cyber threats. Some of these organizations included the U.S. Department of Homeland Security and the Federal Bureau of Investigation. In approximately June of 2017, this exercise was made public and became a national news story. DCED also participated in a cyber-security conference call on October 19, 2016 with these organizations and the Texas Secretary of State. In one of the first news article regarding Dallas County's involvement, published by the Dallas Morning News on June 14, 2017, Pippins-Poole and Dallas County IT Director, Stanley Victrum are quoted as sources. Pippins-Poole is quoted as stating clearly, ***"They didn't infiltrate our system,"…."They couldn't get in."*** Mr. Victrum is credited with stating:

> *Dallas County blocked the IP addresses that the feds provided, said Stanley Victrum, the county's chief information officer. Since 2014, the county has spent $1.23 million on cybersecurity upgrades such as encryption enhancement, antivirus tools and scanners. The county spends an additional $566,000 each year on maintenance, operation and staff salaries for its IT security team, Victrum said.*
> *"We have foreign players that try to come in all the time — almost every day," Victrum said. "The county Commissioners Court has made some pretty significant investments so that we could be safe."*

The Elections Administrator, Pippins-Poole never stated that the Dallas County voting and elections computers, registration, election night reporting and/or other internet-connected

systems were hacked or breached in any way. They were not. It was also reported that Pippins-Poole declined to be interviewed. That is incorrect; Pippins-Poole has always made herself available to discuss the operations of the Elections Department, and help ensure the public integrity of the voting process. What is clear is that unknown actors did probe the County's IT infrastructure. Simply seeing traffic from a system does not mean intrusive hacking is occurring. It is difficult to determine what activities are malicious. In a ***Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security***, dated October 7, 2016, the USIC and the Department of Homeland Security assessed that it would be difficult for someone to alter actual ballot counts or election results by a cyber attack or intrusion because of the de-centralized nature of our election system.

Notwithstanding the above, the overwhelming intelligence behind our preparation and response, however, indicated that the probing by suspicious IP addresses was to target elections and voting resources. In fact, as only as recently as Friday, September 22, 2017 did the U.S. Department of Homeland Security inform (by conference call) approximately 21 states that they had been the subject of attempted intrusions. The Department stated that they did inform those who had "ownership" of the affected systems.

Within the last ten days various news and media sources have verified and made clear, that foreign actors did attempted to compromise and or disrupt the elections and voting process and systems within Texas and the United States:

- "**Russian hackers tried to compromise Texas in presidential election, officials confirm**"; http://www.star-telegram.com/news/politics-government/article174926896.html#storylink=cpy, dated 9/22/17;

- "**Hackers targeted Texas secretary of state website, official says**"; http://www.statesman.com/news/hackers-targeted-texas-secretary-state-website-official-says/7XQbmyh6msawwmX7aJNWDP/?, dated September 22, 2017 by The Statesman;

- "**Homeland Security officials said in September that hackers believed to be Russian agents had targeted voter registration systems in more than 20 states**"; http://keranews.org/post/10-months-after-election-day-feds-tell-states-more-about-russian-hacking 10 Months After Election Day, Feds Tell States More About Russian Hacking, dated 9/23/17 by KERA News

Based on this information, it is evident that Dallas County did everything it could to safeguard the electoral process in the November of 2016 Presidential Election, and did not suffer a breach, "hack" or show of vulnerabilities to our systems as some other local and state authorities did.

DCED is statutorily charged with safeguarding the legal and procedural process and infrastructure of voting in elections for Dallas County. DCED depends on the County's IT Department resources to make sure voting and election related systems and information are protected from threats. To that end, in June 2017, Dallas County hired a new Chief Information Security Officer to manage the review process and duly reflecting current applicable compliance requirements, regulatory and industry best practices in the information security policy.

Dallas County is committed to good cybersecurity and best practices is important for protecting voter registration, election night reporting and other internet connected election systems. DCED and Dallas County will continue to improve and strengthen our voting and elections software, equipment, information and systems, and continue to guard against cyber-threats. We will also continue to provide the public and the media with the facts and information it needs to be assured of these resources.

Media Contact Information:

Toni Pippins-Poole, CERA, CCPA
Elections Administrator
tpippins@dallascounty.org

Robert Heard Sr.
Assistant Elections Administrator
robert.heard@dallascounty.org

# # #