Joint DHS and ODNI Election Security Statement

Friday, October 07, 2016

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

October 07, 2016

Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security

The U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations. The recent disclosures of alleged hacked e-mails on sites like DCLeaks.com and WikiLeaks and by the Guccifer 2.0 online persona are consistent with the methods and motivations of Russian-directed efforts. These thefts and disclosures are intended to interfere with the US election process. Such activity is not new to Moscow—the Russians have used similar tactics and techniques across Europe and Eurasia, for example, to influence public opinion there. We believe, based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities.

Some states have also recently seen scanning and probing of their election-related systems, which in most cases originated from servers operated by a Russian company. However, we are not now in a position to attribute this activity to the Russian Government. The USIC and the Department of Homeland Security (DHS) assess that it would be extremely difficult for someone, including a nation-state actor, to alter actual ballot counts or election results by cyber attack or intrusion. This assessment is based on the decentralized nature of our election system in this country and the number of protections state and local election officials have in place. States ensure that voting machines are not connected to the Internet, and there are numerous checks and balances as well as extensive oversight at multiple levels built into our election process.

Nevertheless, DHS continues to urge state and local election officials to be vigilant and seek cybersecurity assistance from DHS. A number of states have already done so. DHS is providing several services to state and local election officials to assist in their cybersecurity. These services include cyber "hygiene" scans of Internet-facing systems, risk and vulnerability assessments, information sharing about cyber incidents, and best practices for securing voter registration databases and addressing potential cyber threats. DHS has convened an Election Infrastructure Cybersecurity Working Group with experts across all levels of government to raise awareness of cybersecurity risks potentially affecting election infrastructure and the elections process. Secretary Johnson and DHS officials are working directly with the National Association of Secretaries of State to offer assistance, share information, and provide additional resources to state and local officials.

Newsroom Categories

- Recent News
- Reports & Publications
- Press Releases
- Speeches & Interviews
- Congressional Testimonies
- Featured Articles
- IC in the News

Archive

- 2016
- 2015
- 2014
- 2013
- 2012
- 2011
- 2010
- 2009
- 2008
- 2007
- 2006
- 2005