Press Office
U.S. Department of Homeland Security

Press Release

January 6, 2017

STATEMENT BY SECRETARY JEH JOHNSON ON THE DESIGNATION OF ELECTION INFRASTRUCTURE AS A CRITICAL INFRASTRUCTURE SUBSECTOR

I have determined that election infrastructure in this country should be designated as a subsector of the existing Government Facilities critical infrastructure sector. Given the vital role elections play in this country, it is clear that certain systems and assets of election infrastructure meet the definition of critical infrastructure, in fact and in law.

I have reached this determination so that election infrastructure will, on a more formal and enduring basis, be a priority for cybersecurity assistance and protections that the Department of Homeland Security provides to a range of private and public sector entities. By "election infrastructure," we mean storage facilities, polling places, and centralized vote tabulations locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments.

Prior to reaching this determination, my staff and I consulted many state and local election officials; I am aware that many of them are opposed to this designation. It is important to stress what this designation does and does not mean. This designation does not mean a federal takeover, regulation, oversight or intrusion concerning elections in this country. This designation does nothing to change the role state and local governments have in administering and running elections.

The designation of election infrastructure as critical infrastructure subsector does mean that election infrastructure becomes a priority within the National Infrastructure Protection Plan. It also enables this Department to prioritize our cybersecurity assistance to state and local election officials, but only for those who request it. Further, the designation makes clear both domestically and internationally that election infrastructure enjoys all the benefits and protections of critical infrastructure that the U.S. government

has to offer. Finally, a designation makes it easier for the federal government to have full and frank discussions with key stakeholders regarding sensitive vulnerability information.

Particularly in these times, this designation is simply the right and obvious thing to do.

At present, there are sixteen critical infrastructure sectors, including twenty subsectors that are eligible to receive prioritized cybersecurity assistance from the Department of Homeland Security. The existing critical infrastructure sectors are:

Chemical
Commercial Facilities
Communications
Critical Manufacturing
Dams
Defense Industrial Base
Emergency Services
Energy
Financial Services
Food and Agriculture
Government Facilities
Healthcare and Public Health
Information Technology
Nuclear Reactors, Material, and Waste
Transportation Systems
Water and Wastewater Systems

Entities within these sectors all benefit from this designation and work with us closely on cybersecurity. For example, we have developed joint cybersecurity exercises with numerous companies within the communications, information technology, financial services and energy sectors to improve our incident response capabilities. We have also streamlined access to unclassified and classified information to critical infrastructure owners and operators in partnership with information sharing and analysis organizations. Moreover, many critical infrastructure sectors include assets and systems owned and operated by state and local governments, such as dams, healthcare and public health, and water and wastewater systems.

Now more than ever, it is important that we offer our assistance to state and local election officials in the cybersecurity of their systems. Election infrastructure is vital to our national interests, and cyber attacks on this country are becoming more sophisticated, and bad cyber actors – ranging from nation states, cyber criminals and hacktivists – are becoming more sophisticated and dangerous.

Further, our increasingly digital and connected world has reshaped our lives. It has streamlined everyday tasks and changed the way we communicate. But, just as the continually evolving digital age has improved our quality of life, it has also introduced an array of cyber threats and implications.

Cybersecurity continues to be a top priority for DHS, as it is for state and local election officials across the country. This designation enables the states, should they request it, to leverage the full scope of cybersecurity services we can make available to them.

###