STATEMENT

Statement of
Commissioner Neil Chatterjee on
Cyber Security Incident Reporting Reliability Standards

Date: July 19, 2018

Item Nos.: E-1
Docket No. RM18-2-000

"Protecting our nation's electric grid from cyber security threats is one of the Commission's most pressing challenges. Both the Department of Homeland Security and Federal Bureau of Investigation have issued multiple public reports describing intrusion campaigns by Russian government cyber actors against our critical infrastructure, including the electric grid. While thankfully none of these intrusions have resulted in an actual power outage, they do represent an unsettling uptick in attempts to undermine America's critical infrastructure systems.

"I am deeply concerned by these threats as our adversaries continue to grow only bolder and more sophisticated with each passing day. That's why I've been an outspoken proponent of working with both industry and our government partners to do what we can to better defend against potential intrusions. The record before us similarly reflects these concerns and reveals that inaction is not a feasible or responsible option. The Commission has a statutory obligation to act. I believe it's imperative that we ensure our colleagues at the North American Reliability Corporation and DHS have adequate information to understand the evolving threat landscape for industrial control systems.

"While it's critical that we take decisive action to address growing cyber threats, I recognize that implementing mandatory reliability standards, if not done properly, could place significant financial and organizational burdens on industry with little practical benefit. I support today's final rule because it provides NERC an appropriate measure of flexibility to work with industry stakeholders to ensure that it and DHS receive the timely, accurate, and actionable information they need without dictating an overly prescriptive and burdensome approach. And I encourage industry stakeholders to engage responsibly and actively in that reliability standards development process to ensure that the result entails a compliance burden that is manageable and proportionate to the cyber threats to our nation's critical infrastructure."