



CISA
CYBER+INFRASTRUCTURE

March 26, 2019

STATEMENT FOR THE RECORD - BOB KOLASKY, DIRECTOR, NATIONAL RISK MANAGEMENT CENTER, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, DHS

FEDERAL ENERGY REGULATORY COMMISSION AND THE UNITED STATES DEPARTMENT OF ENERGY – SECURITY INVESTMENTS FOR ENERGY INFRASTRUCTURE TECHNICAL CONFERENCE

Good morning. I appreciate FERC extending the opportunity for me to speak here today and to share my perspective on our shared mission to enhance the resilience of the Nation's energy infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA) acts as the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure to secure tomorrow. The National Risk Management Center (NRMC) within CISA, of which I'm privileged to lead, is a planning, analysis and collaboration center working to identify the most strategic threats to our Nation's critical infrastructure. Our efforts focus on two lanes of activity – analysis of critical infrastructure risk, and initiative planning and execution to combat those risks. I will highlight some of these efforts today.

Cyber threats remain one of the most significant strategic risks for the United States, threatening our national security, economic prosperity, and public health and safety. The past several years have marked a turning point in the cyber domain, at least in the public consciousness. We have seen advanced persistent threat actors, including hackers, cyber criminals, and nation-states increase the frequency and sophistication of these attacks. Our adversaries have been developing and using advanced cyber capabilities in attempts to undermine critical infrastructure, target our livelihoods and innovation, steal our national security secrets, and threaten our democracy.

Risk is increasingly cross-sector in nature. A silo-ed approach to risk identification and management will simply not work. By the nature of the threat, and infrastructure design, risk transcends infrastructure sectors, is shared across state and national lines, and is held by both government and industry. We need to look no further than NotPetya, the most costly cyber-attack in history - which we have attributed to Russia - to see how risk easily jumps across sectors and continents and how it can hit private sector organizations particularly hard. All of us in this room have a role to play, and I appreciate the ongoing partnership from DOE, FERC, and our private sector partners.

National Critical Functions

Historically, the U.S. government has focused on prioritizing critical infrastructure from the perspective of assets and organizations. A different approach for prioritization is needed to better address system-wide and cross-sector risks and dependencies. CISA, through the NRMC, is leading an effort to develop a set of National Critical Functions to guide critical infrastructure risk management.

National Critical Functions are defined as “the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on national security, economic security, national public health or safety, or any combination thereof.”

This construct forces a risk management conversation that is less about what an entity is as a business or government, and more about what an entity does and what it enables. This framework allows us to analyze issue sets in the risk management space not in isolation, but with a more holistic context.

Defense Critical Electric Infrastructure (DCEI)

A relevant example of this functional approach to risk in action is our current DCEI initiative between DHS, DOE, and DOD. The NRMC has developed military base dependencies on functions provisioned by the critical infrastructure community. This effort right now is focusing mostly on electricity but we have plans to expand it to functions produced by the Communications Sector as well. By using this National Critical Functions lens first, our risk analysis then enables resilience building in a strategic and prioritized way for key defense assets. The partnership and ongoing evolution of this initiative bode well for sustained collaboration to reduce risk – cyber and otherwise – to our Nation’s critical infrastructure.