##### November 26, 2012

**TO:** All Interested Parties

**FROM:** Jonathan Booe, NAESB Deputy Director

**RE: Cyber Security Update**

**Update Cyber Security Efforts –**

In the months of October, November and December, the Department of Energy and the Department of Homeland Security (DHS) are hosting a series of regional classified and unclassified briefings to discuss the recent cyber security attacks on the energy sector. During these meetings representatives from the FBI and the DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) are reviewing the malware attacks on Telvent, Saudi Aramco and RasGas and discussing potential mitigation and best practices that could have been employed to combat against such attacks. This effort undertaken in addition to a number of communications - as recent as November 20 – from several members of congress calling for the development comprehensive cyber security legislation to support the protection of the energy sector from cyber threats. In response to the increased scrutiny on cyber security, it has been proposed that NAESB develop two fact sheets related to NAESB standards and work products that related to cybersecurity for the natural gas and electricity markets.