

From: <Martin>, Tony W <twmartin@babcock.com>
Date: Friday, April 5, 2013 12:18 PM
To: cyberframework <cyberframework@nist.gov>
Subject: Developing a Framework to Improve Critical Infrastructure Cyber Security

Diane Honeycutt,

I am the Manager of Information Security for The Babcock & Wilcox Company. I support establishing a common framework that applies a graded approach to security with the level of protections commensurate with the value of the asset to be protected and risk to that asset. In my opinion, NIST should consider adopting the SANS 20 Critical Security Controls for Effective Cyber Defense with emphasis on implementing the Australian 4, (white listing, patching of systems, patching of applications, and limiting privileged access). I've found this to be the most effective way to implement cyber security because it takes a pragmatic and cost-conscious approach to get the most benefit from the resources invested in security. The SANS 20 Critical Controls helps organizations on a tight budget with limited staffing to prioritize security initiatives in a manner that provides the maximum protection possible against the most significant threats. However, it also has enough depth to guide the implementation of continuous improvements as an organization progresses to greater levels of maturity in their security program.

Tony W. Martin, CISSP-ISSAP
Manager, Information Security
B&W ITSC

This message is intended only for the individual or entity to which it is addressed and contains information that is proprietary to The Babcock & Wilcox Company and/or its affiliates, or may be otherwise confidential. If the reader of this message is not the intended recipient, or the employee agent responsible for delivering the message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify the sender immediately by return e-mail and delete this message from your computer. Thank you.