From: John DiMaria
Sent: Monday, January 1, 2018 8:15 PM
To: cyberframework <cyberframework@nist.gov>
Subject: BSI Comments on the Cybersecurity Framework Draft Version 1.1

BSI applauds NIST for their continued quest to meet the objectives of continual improvement and international harmonization. This new draft is a prime example of both. While there are a number of areas of improvement, below are the ones that stand out as having the most significant impact and have been part of the foundation of cybersecurity in the international world.

Cyber-Attack Lifecycle

With the large volumes of data thrown at us every day and the continued attacks, threat intelligence is becoming a very significant factor in the protection of an organization in mitigating risk.

Cyber Supply Chain Risk Management (we call this supplier relationships)

Risks associated with interdependencies throughout the supply chain. You are only a strong as your weakest link

Measuring Cybersecurity

Probably the most significant

Every control is a cost to the organization, so you need to maximize the value and effect for its cybersecurity investments. This meets a few significant objectives:

- Reducing risk by making sure the controls you have in place are justified and effective
- Ensure there are clear measurable objectives and planning to achieve them
- And answers to the one sticking point of “cost effectiveness” Metrics facilitate measuring cost effectiveness and ensuring that objective is being met.

John A DiMaria; CSSBB, HISP, MHISP, AMBCI, CERP, CSA Research Fellow
Global Product Champion for Information Security and Business Continuity