From: Giles, Anthony
Sent: Thursday, January 18, 2018 11:30 AM
To: cyberframework <cyberframework@nist.gov>
Subject: NSF Comments Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 Draft 2

Andrea Arbelaez
National Institute of Standards and Technology
100 Bureau Drive
Mail Stop 2000
Gaithersburg, MD 20899

Good Morning Andrea,

Thank you for the opportunity to make comments on the revised Framework for Improving Critical Infrastructure Cybersecurity. I appreciate and like the continued focus and, direction on managing cybersecurity risks with a clear understanding of the organizations business drivers and security considerations specific to the required technology an organization may/may not use. I worked to stay focused on addressing changes in the current cybersecurity ecosystem.

Comments Include:

- 4.0 Self-Assessing Cybersecurity Risk with the Framework:
    - The focus on objectives and frameworks included in the section could cause confusion.
        - The way the section is worded it is very difficult to measure objectives without a common framework or controls matrix
            - Table 2: Framework Core starts to establish a framework but, there are 6 varying informative references
                - Just two of the Frameworks NIST 800-171 and ISO 27001 have appendix controls for risk and those two controls differ slightly
                    - There could be some consideration given to a review of ISO 31000 Implementing Risk Management
                        - We should work together looking at the 6 frameworks to establish potential common benchmarks. The benchmarks can enable or, provide organizations with a structure to make a decision.
- Table 2 Framework Core: Data Security (PR.DS)
    - PR.DS-1 and PR.DS-2 – Data-at-rest is protected and Data-in-transit is protected
        - The requirements could better align with the NIST controls in place Appendix D 3.8.6. This would support the implementation of a cryptographic mechanism
            - With data in transit I don't think the framework is keeping up with the pace of potential social attacks that could take place after data leaves a facility

        - Unencrypted drives could remain open for SATA Cable access or become lost in transit with useable data
- Table 2 Framework Core: Awareness and Training (PR.AT)
    - PR.AT-1 – All users are informed and trained
        - The people segment of cybersecurity is continuing to be one of the highest risks
            - I think in staying up to date with current threats we need to spend more time building our awareness and training controls
                - This can include training on social engineering or phishing attempts
- Table 2 Framework Core: Security Continuous Monitoring (DE.CM)
    - DE.CM-2 – monitoring of the physical environment
        - This is also an area that is high risk for social attacks
            - Standards struggle to define what it means to monitor a physical environment

Thank you for the opportunity to comment. I look forward to seeing the revised draft.

If there is future opportunity to sit on framework development committees I would be very interested in doing so.

Thank you again for your time and consideration.

Thank You,

Tony Giles | ISO 27001:2013 Information Security Management Systems Lead Auditor and Director, Custom Audit Programs - ISR