Response to:

RFI - Framework for Reducing Cyber Risks to Critical Infrastructure

Washington Metropolitan Area Transit Authority
Office of IT Security
POC: Adam Meyer CISO

Introduction:

The Washington Metropolitan Area Transit Authority (WMATA) is the second largest mass transit system in the country. The Authority was created in 1967 by an Interstate Compact to plan, develop, build, finance and operate a balanced regional transportation system in the National Capital area and currently serves a population of 3.5 million within a 1,500 square-mile area.

Background:

Due to the infrastructure in operation by WMATA and its service area of the national capital region, the authority is in a unique position to provide feedback on the potential impacts of the Cyber Security Executive Order since it is a single organization that interacts with every Federal, State, local and private jurisdiction in the national capital region on a daily basis. Additionally, due to WMATA's significant investment in technology coupled with its mission as public transit, operation as a public service but a private entity, and need to interoperate with two states, the District of Columbia and the Federal Government we are exposed to a substantial cyber security regulatory environment that appears to be uncommon when in comparison to many of your other stakeholders.

Methods:

Since the very technologies that empower us to lead and create also empower those who would disrupt and destroy. WMATA has taken a Cyber Security approach that is rooted through the lens of Business Resiliency rather than a culture of compliance as compliance does not result in good security but good security does result in compliance. It is our opinion and strategic direction to deploy countermeasures based on a capability maturity model construct versus a method based on "Control Compliance"

We also identified that the issue in not necessarily a lack of published frameworks or standards but rather the management infrastructure that selects, implements and monitors how countermeasures are deployed to reduce our risk and liability exposure. To accomplish this, the authority has selected the CERT Resiliency Management Model (CERT-RMM) as the management framework to measure capability within the Cyber organization based on a standard set of goals. The primary intent is to improve confidence in how the organization responds in times of operational stress. In addition to the CERT-RMM Model, we have selected other core best practices such as the CAG Top 20 controls due to the common knowledge of the controls, known effectiveness of the controls and robust vendor base that supports it which creates instances of waste elimination, and enables active monitoring and measurement for continuous improvement. Lastly we will be re-using the philosophy that was published by the U.S. State departments IPost initiative of creating measurable weighting factors based on a well thought out algorithm and sharing those results with senior leaders.

Feedback:

It is our opinion that sufficient frameworks already exist that can be leveraged for this effort. The key considerations should be the overarching management processes that implement and measure the effectiveness of deployed countermeasures for effectiveness based on a maturity level. Therefore it is our recommendation that the following high level frameworks and philosophies be strongly considered in the development of this framework:

Tool and Frameworks

Overarching Management Framework - Carnegie Mellon CERT Resiliency Management Model (CERT-RMM)

Core Countermeasures – SANS Top 20 Controls

IPost Measurement Style – Assesses an organization based on communities of interest and increase weight factors for critical controls such as the top 20

Philosophies:

1. Resiliency Maturity and not Control Compliance
2. Compliance does not result in good security but good security does result in compliance
3. Deployed countermeasures should directly map to identifiable liability reductions for the organization.
4. Do not reduce security in the name of security, be mindful of all the other cyber centric burdens of the organization such as Privacy, HIPPA, Safety, Financial, PCI as creating a new framework redirects labor resources from one area to another and may take away from stopping the bleeding.
5. The CERT-RMM/Top 20 framework is repeatable, measurable and effective as well as cost advantageous