National Cyber-Forensics and Training Alliance
2000 Technology Drive, Suite 450, Pittsburgh, Pennsylvania 15219
Tel. (412) 802-8000, ext. 236 Fax (412) 802-8510 http://www.ncfta.net

Public Comment for Developing a Framework to Improve Critical Infrastructure Cybersecurity

Introduction

With the Executive Order "Improving Critical Infrastructure Cybersecurity" issued by President Obama and the Notice; Request for Information provided by NIST, a "new normal" is coming to light within the public, private, and academic sectors. Following these documents, workshops, and ultimately a final framework will be providing better guidelines and methods to secure all sectors deemed critical infrastructure. NCFTA believes an all angles approach will yield the best results for the final draft.

In order to be successful, all voices must be heard from each sector. The public comments and subsequent workshops will be orchestrating this movement into wide spread communication for the common good of securing both physical and virtual assets of the nation's critical infrastructure. NCFTA is taking immense interest of these communications from the Executive Order and RFI in order to offer its communication services to the effort of getting each of these sectors to communicate.

NCFTA is a nonprofit 501c 3 organization specializing in building cross-sector trusted relationships that enables effective communication platforms to share information.

Current Risk Management Practices

The greatest challenge of securing both virtual and physical critical infrastructure is enabling the data sharing and collaboration that is needed. The ultimate goal is protect every network. This requires habitual face time meetings in order to establish trust and knowledge of each sector. Often times a threat is not singular. It can be seen hitting the same industry/sector at the same time or within a designated time. Early warnings and collaborations would be able to prevent a threat from perpetrating an entire sector. NIST and critical infrastructure entities need to also consider that a risk may hit multiple industries at once. Frequently, industries are being hit with the same threat, however since communication across sectors is not a common response action, the threat is measured in each industry individually and not collectively in order to produce a clearer threat assessment.

This example can also be seen in the public sector. Law Enforcement needs to collaborate with each other in order to deconflict and avoid duplication of efforts. Establishing a neutral common ground organization for Law Enforcement, Private, and Public, to head up these meetings and keep the level of contribution equal will ultimately lead to identifying current risks with effective solutions.

Ultimately, data sharing is most effective when a collaborative relationship can be built over time in a neutral venue. Entities are able to earn trust and honor trust with this model.

The framework needs to focus on what can be shared and not concentrate on what cannot be shared.

NCFTA recommends:

- Establish a neutral, collaborative venue for all willing and active public, private, and academic participants to build relationships for information and threat sharing
- Provide legislation solutions to allow for data sharing without liability
- Focus on data sharing abilities

Use of Frameworks, Standards, Guidelines, and Best Practices

Upon establishing the final draft of the framework, NCFTA would like to see a living framework that is regularly updated and reviewed. When creating a framework that overlaps multiple industries, the framework needs to be risk based, outcome based, flexible, and measurable.

The finished product should be clear and concise even to a non technical audience. A support model should also be established with resources that can be accessible to all. This voluntary program and subsequent framework will only be successful if it is used and accepted by the industry that utilizes it the most.

When building a guideline for data sharing across sectors, a clear method and process must be established when sharing declassified and unclassified documents from the following: LE, government, industry, and academia. Data sharing and threat assessments cannot be a one sided affair. Data sharing should also be preventive and proactive not reactive.

NCFTA recommends:

- Establish a framework and process to update regularly
- Finish framework with non technical rhetoric
- Support framework with “how to” resources
- Create data sharing process for all concerned entities with time sensitivity in mind

Overall Recommendations for Success

NCFTA would like to point out the following additional items to consider when formulating the framework:

- Clearly define critical infrastructure
- Define buzz term “cybersecurity” as it relates only to framework
- Keep the small/medium/enterprise needs in mind when formulating the framework

Conclusion

NCFTA is looking forward to NIST’s upcoming workshops on formulating this framework and to offer its knowledge when it comes to data sharing and collaborating in order to protect critical infrastructure.