Houston Urban Area Security Initiative (UASI)

Cybersecurity Mini-Assessment Workshop

3 June 2016

Agenda

UASI Introduction	10:00AM - 10:30AM
Cyber Security Mini-Assessment	10:30AM - Noon
Networking Lunch	Noon - 1:30PM
UASI Cyber Tools Overview	1:30PM - 3:30PM

- ✓ Cybersecurity Control Implementation Interface (CCII)
- ✓ Cybersecurity Posture Dashboard
- ✓ Cyber Disruption Readiness Assessment Tool

Houston Urban Area Security Initiative (UASI)

Since 2003, the greater Houston area has been considered by the Department of Homeland Security (DHS) to be among the highest threat urban areas in the nation.

The purpose of the Houston Urban Security Initiative (UASI) and its Area Workgroup (UAWG) is to improve the region’s capacity to **prevent, protect against, respond to, and recover from acts of terrorism or other major disasters** through the successful implementation of the *Houston Urban Area Homeland Security Strategy*.

How Did We Get Here?

In April 2014 the City of Houston (COH) launched a cyber security project to identify the risk posture of COH systems and networks.

Using an established and comprehensive framework was the best approach.

National Institute of Standards & Technology (NIST) Cybersecurity Framework was selected to be the Cybersecurity Framework of choice.

NIST Cybersecurity Framework used as a guide along with other governmental and industry best practice subject matter to address Federal, State and Local regulatory requirements.

NIST Cybersecurity Framework consists of vast amounts of information that was turned into 800+ questions throughout the Eighteen (18) control families and casts the discussion and details of cybersecurity in the vocabulary of risk management.

The Framework

The Framework was created through collaboration between industry and government and consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk.

The Framework consists of vast amounts of information culled from standards, guidelines and best practices. A process was created that would allow a user of the Framework to answer questions to determine their risk posture. The framework casts the discussion and details of cybersecurity in the vocabulary of risk management.

Approximately 800 questions (based largely on NIST 800-53) throughout, Eighteen (18) control families, including Management, Operational and Technical, make up the assessment process of the Framework.

A Source to Share

Risk Assessment is an Iterative & Continuous Process

It became evident that having a tool that would provide guidance and a repeatable process would be helpful to the City as well as to regional partners needing to perform similar assessments.

The program team made the decision to create a shareable, and scalable cybersecurity package of best practice documentation and utilities that can be utilized in all organizations regardless of size.

The result was the creation of the Cybersecurity Control Implementation Interface (CCII). The interface provides access to:

- ✓ Policies and Procedures Boilerplates
- ✓ Implementation Best Practices
- ✓ Interactive Assessment Utilities
- ✓ A Step-by-Step Roadmap
- ✓ FAQ’s

Web-based Application & Tools

The CCII Tool has been structured to support online or offline access:

- ✓ Content and tool source code are available for download
- ✓ Notifications of any changes and uploads automatic to registrants

Tool is continually being enhanced as we move through program stages of the program. To date the items that are under development encompass activities associated with mitigation planning and actions:

- ✓ Processes and Methodologies
- ✓ Standards and Procedure Boilerplates
- ✓ Interactive Tool to prioritize mitigations based on:
  - ➢ Impact – Risk – Difficulty – Time – Cost
- ✓ Mitigation Impact Cycle Approach
- ✓ Monitored Event Action Plan

Cybersecurity Mini-Assessment

The mini cyber assessment is a pre-assessment tool that will compare, at a high-level, based on your response to a set of questions related to specific controls how your Cybersecurity program/practices rate against the NIST Cybersecurity Framework.

The report generated from this tool is weighted based on the NIST priorities and displays results based on your most prevalent weaknesses from your direct responses to questions presented in the assessment.

The objective of this mini-assessment is to provide organizations a level of insight on which controls to address in what order based on the organizations business goals.

Cybersecurity Mini-Assessment Registration

To register for the mini cyber assessment please navigate to:

https://cciidashboard.info

Complete the requested information with the following access code:

629304

Cyber Tools Overview

Cybersecurity Control Implementation Interface (CCII)

https://www.cciitool.info/

Cybersecurity Posture Dashboard

http://pdash.bonustool.com/

Cyber Disruption Readiness Assessment Tool

https://www.cyberdisruptionplanning.com

How Do You Get Involved?

Go to https://www.cciitool.info and register!

- ✓ Download the Documents and Artifacts
- ✓ Post Questions (we will respond!)
- ✓ Post Suggestions (we love feedback!)

Let us know how we are doing!

Theresa G. Blackwell, Executive Consultant
Virtuo Group Corporation
tblackwell@virtuogroup.com or theresa.blackwell@houstontx.gov

David LaPlante, CISO
City of Houston
david.laplante@houstontx.gov

Next Steps & Logistics

Questions?