U.S. Department of Health and Human Services

CSA Section 405(d) Workshop #1

AGENDA

Monday, May 22 – Tuesday, May 23, 2017

WORKSHOP GOALS:

1. Commence the development of a cybersecurity Guidance for the Healthcare and Public Health Sector as mandated by Section 405(d) of the 2015 Cybersecurity Information Sharing Act.
2. Inform participants about the goals and objectives of the CSA 405(d) Task Group, HHS' proposed scope of the Guidance, the value to each participant, the process by which the Guidance will be developed, final outcomes and follow-up activities.
3. Develop a prioritized list of assets (people, processes, technologies, and data) that are essential for the successful performance of healthcare operations.

Monday, May 22

8:30 AM – 9:00 AM Registration & Check-in

PLENARY SESSION (Room 800, Hubert H. Humphrey Building)

9:00 AM – 9:10 AM Introduction and Workshop Overview

Julie Chua
HHS Security Risk Management Division Manager
Office of Information Security (OIS)
HHS Office of the Chief Information Officer (HHS OCIO)

Stephan Smith
Support to HHS OCIO/OIS

9:10 AM – 9:20 AM Welcome Remarks

Chris Wlaschin
Chief information Security Officer
HHS

9:20 AM – 9:50 AM Background and Overview of the CSA Section 405(d) Cybersecurity Guidance (v1.0)

Julie Chua
HHS OCIO/OIS

TIMES AND SCHEDULE SUBJECT TO CHANGE

Stephan Smith
Support to HHS/OCIO/OIS

9:50 AM – 10:00 AM BREAK

10:00 AM – 11:30 AM Panel Discussion (CIPAC OPEN)

Description: This panel will discuss the need for common sense, implementable, and practical cybersecurity guidance for the Healthcare and Public Health Sector, starting with the healthcare provider community; the challenges healthcare providers face with securing their assets given the latest cyber threats to the healthcare sector; and how the cybersecurity guidance the task force is developing could help address these challenges.

Moderator: Julie Chua
Security Risk Management Division Manager
HHS Office of the Chief Information Officer
Office of Information Security

Panelists: Matthew Barrett
National Institute of Standards and Technology
Cybersecurity Framework Lead

Erik Decker
University of Chicago Hospital
Chief Information Security Officer

Eric Goldstein
Department of Homeland Security/Cybersecurity and Communications Branch
Chief, Partnerships and Engagement

Kendra Siler-Marsiglio
CommunityHealth IT
President/CEO

Karl West
Intermountain Healthcare
Chief Information Security Officer and Assistant Vice President

Chris Wlaschin
HHS Office of the Chief Information Officer/Office of Information Security/Chief Information Security Officer

TIMES AND SCHEDULE SUBJECT TO CHANGE

11:30AM – 12:30 PM ***LUNCH (Non-Hosted; Humphrey Building Cafeteria or Local Establishments)***

12:30-1:00 PM Process through Security at Thomas P. O'Neill Jr. Federal Building

1:00 PM – 4:00 PM FACILITATED BREAKOUT SESSIONS (Thomas P. O'Neill Jr. Federal Building)

Description: Workshop participants will each be assigned to a breakout group consisting of approximately 25-30 participants. . We estimate an approximately total of 2-3 breakout groups, which will meet during both days. Breakout groups will: 1) identify key healthcare assets; 2) describe the attributes of these assets; 3) deliberate on the impact of these assets being compromised due to cyber incidents; 4) establish criteria by which these assets should be prioritized; and 5) prioritize the identified assets based on the established criteria.

1:00 PM – 2:20 PM **Breakout Session I**

Participants will identify and develop a list of assets and the functions that are of primary concern to healthcare providers. These will serve as the first set of assets/asset categories, on which the CSA Section 405(d) Cybersecurity Guidance will focus.

2:20 PM – 2:30 PM **BREAK**

2:30 PM – 4:00 PM **Breakout Session II**

Participants will begin to deliberate the following aspects of the assets identified during Breakout Session I:

- Asset components Interdependencies;
- Security risks involved with asset;
- Regulatory and compliance considerations
- Impact of cyber incidents on asset; and
- Similar assets

4:00 PM **Adjourn (CIPAC CLOSE)**

TUESDAY, MAY 23

8:30 AM Registration & Check-in (Museum of the American Indian)

BREAKOUT SESSIONS (Museum of the American Indian)

TIMES AND SCHEDULE SUBJECT TO CHANGE

9:00 AM – 10:20 AM **Breakout Session III (CIPAC OPEN)**

Participants continue to deliberate the following aspects of the assets identified during Breakout Session I:

- Asset components;
- Interdependencies;
- Security risks involved with asset;
- Regulatory and compliance considerations
- Impact of cyber incidents on asset; and
- Similar asset/assets

10:20 AM – 10:30 AM **BREAK**

10:30 AM – 12:00 PM **Breakout Session IV**

Participants complete deliberation of the attributes of the assets identified during Breakout Session I and conduct brief prioritization of the assets discussed during the two days' breakout sessions

12:00 PM – 1:00 PM ***LUNCH (Non-Hosted; Museum of the American Indian Cafeteria or Local Establishments)***

PLENARY SESSION (Museum of the American Indian)

1:00 PM – 2:00 PM **Asset Prioritization**

Participants will prioritize the assets identified during Breakout Session I based on criteria determined by the Group.

2:15 PM – 2:30 PM **Break**

2:30 PM – 3:00 PM **Workshop Summary & Closing Remarks**

- What was discussed? What was discovered?
- What are the general impressions from the 2 days?
- Next steps

Facilitators:

Nickol Todd
HHS Office of the Assistant Secretary for Preparedness and Readiness (ASPR)

Julie Chua
HHS OCIO/OIS

Stephan Smith
Support to HHS/OCIO/OIS

3:00 PM **ADJOURN (CIPAC CLOSE)**

TIMES AND SCHEDULE SUBJECT TO CHANGE