

# National Protection and Programs Directorate Cyber Incident Data and Analysis Repository Workshop

Anonymous Cyber  
Incident Data

Repository Supported  
Risk Analysis

Tuesday and Wednesday, April 19-20, 2016  
2451 Crystal Drive, Arlington, VA 22202

## CONFERENCE AGENDA

---

### GOALS:

1. Share the findings of the Cyber Incident Data and Analysis Working Group (CIDA WG), which is comprised of cybersecurity professionals from various critical infrastructure sectors, insurance companies, and other private sector organizations on the:
  - a. Value proposition of a cyber incident data and analysis repository (CIDAR);
  - b. Cyber incident data points that could be shared into a repository to support needed analysis; and
  - c. Perceived challenges to sharing data into the repository and overcoming those challenges.
2. Validate the feasibility of/ and solicit support for a CIDAR from the broad cybersecurity community. Receive input on how cyber incident data points shared into a CIDAR should be prioritized, operationalized and automated and how the repository should be executed.
3. Receive input on voluntary information sharing approaches, models and best practices that could inform any future repository implementation.

### TUESDAY, APRIL 19

**8:00 AM – 8:30 AM**

**REGISTRATION**

**8:30 AM – 8:50 AM**

**Introduction and Workshop Overview**

Matt Shabat  
DHS/NPPD

**8:50 AM – 9:30 AM**

**Background and Overview of the CIDA WG, its Key Findings and Conclusions**

Tom Finan  
Chief Strategy Officer  
Ark Network Security Solutions

Cynthia Wright  
MITRE  
Supporting DHS/NPPD

---

**TIMES AND SCHEDULE SUBJECT TO CHANGE**

# CONFERENCE AGENDA

---

9:30 – 9:40 am

## Welcome Remarks

Dr. Phyllis Schneck  
Deputy Under Secretary for Cybersecurity and Communications  
DHS/NPPD

9:50 AM – 10:00 AM **BREAK**

## PLENARY SESSION

**DESCRIPTION:** One of the biggest challenges for repositories is the development of correct metrics and measurements that incentivize a broad array of stakeholders to make contributions. Sharing of sensitive cyber incident data, assured privacy and anonymization, data security, automation and technical design present additional difficulties when creating a widely used repository. This panel will discuss how organizations collect, share and anonymize data as well as lessons learned in metric selection and other decisions made when establishing and managing a data repository.

**(MODERATOR)** Dr. Sandor Boyson, Director of the Supply Chain Management Center and Research Professor at the Robert H. Smith School of Business, University of Maryland College Park

**(PANELISTS)** Financial Services - Information Sharing and Analysis Center  
Rick Lacafta  
Director for Insurance and Content

Aviation Safety Information Analysis and Sharing/Federal Aviation Administration  
Randy L. McGuire  
Department Head, Aviation Safety Analysis

US-CERT  
Tom Millar  
Communications Chief

Cybersecurity Information Sharing Partnership (CiSP), UK-CERT  
Robert Frost  
Head of Strategic Analysis

National Vulnerability Database/National Institute of Standards and Technology  
Harold Booth  
Computer Scientist

12:00 PM – 1:00 PM

## LUNCH

1:00 PM – 4:00 PM **BREAKOUT SESSIONS**

**DESCRIPTION:** CIDAWG participants identified, developed, evaluated and consolidated nearly 30 candidate data categories into a concise list of 16 that, if anonymously shared into a repository, could be used to perform trend and other analyses by enterprise risk owners and insurers. The 16 data categories have been assembled into 4 groups, each containing 4 of the 16 data points. These are: General Incident

---

**TIMES AND SCHEDULE SUBJECT TO CHANGE**

# CONFERENCE AGENDA

---

Information; Consequences and Impacts; Organizational Practices and Maturity; and Incident Response and Recover. Participants will be placed in groups and asked to provide input on each data category.

## **1:00 PM – 2:30 PM      Breakout Session I**

1. General Incident Information
2. Consequences and Impacts
3. Organizational Practices and Maturity
4. Incident Response and Recovery.

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

1. Consequences and Impacts
2. Organizational Practices and Maturity
3. Incident Response and Recovery
4. General Incident Information

## **WEDNESDAY, APRIL 20**

### **PLENARY SESSION**

#### **8:30 AM – 9:00 AM      Recap of the Previous Day and Direction for Today**

#### **9:00 AM – 9:30 AM      Keynote Address**

Adam Isles

Principal, The Chertoff Group

#### **9:30 AM – 9:45 AM      BREAK**

#### **9:30 AM – 11:30 AM      Breakout Session III**

1. Organizational Practices and Maturity
2. Incident Response and Recovery
3. General Incident Information
4. Consequences and Impact

#### **11:30 AM – 12:30 PM      LUNCH**

#### **12:30 PM – 2:00 PM      Breakout Session IV**

1. Incident Response and Recover
2. General Incident Information
3. Consequences and Impacts
4. Organizational Practices and Maturity

---

**TIMES AND SCHEDULE SUBJECT TO CHANGE**

# CONFERENCE AGENDA

---

2:00 PM – 2:30 PM      Workshop Summary / Closing Remarks

2:30 PM – 3:30 PM      CIDAWG meeting under CIPAC

---

**TIMES AND SCHEDULE SUBJECT TO CHANGE**