WELCOME!

UMA Online

TOWN HALL

Bus & Motorcoach NEWS

Today's Agenda

UMA Online TOWN HALL

1—Welcome & Intro
- Scott Michael
- EXPO Sponsor Thank You's
- Welcome New UMA Board Members

2.Legislative & Regulatory Report
- Ken Presley
- Becky Weber

3.Guest Speaker:
Transportation Safety Administration (TSA)

4.EXPO 2023: Orlando, Florida

5.Overdrive
Time to visit with friends

EXPO THANK YOU:

Premium Sponsors

BYD

PREVOST

Mercedes-Benz

Irizar

TEMSA

UMA MOTORCOACH EXPO
RECONNECTING
UMA
February 20-24 | Long Beach, CA

ABC
COMPANIES

MCI

UMA
United Motorcoach Association

Wednesday's Poolside Dinner

Sponsored by:

ABC COMPANIES

MCI

PREVOST

BRIDGESTONE

LANCER INSURANCE
The Difference is Our Attitude.

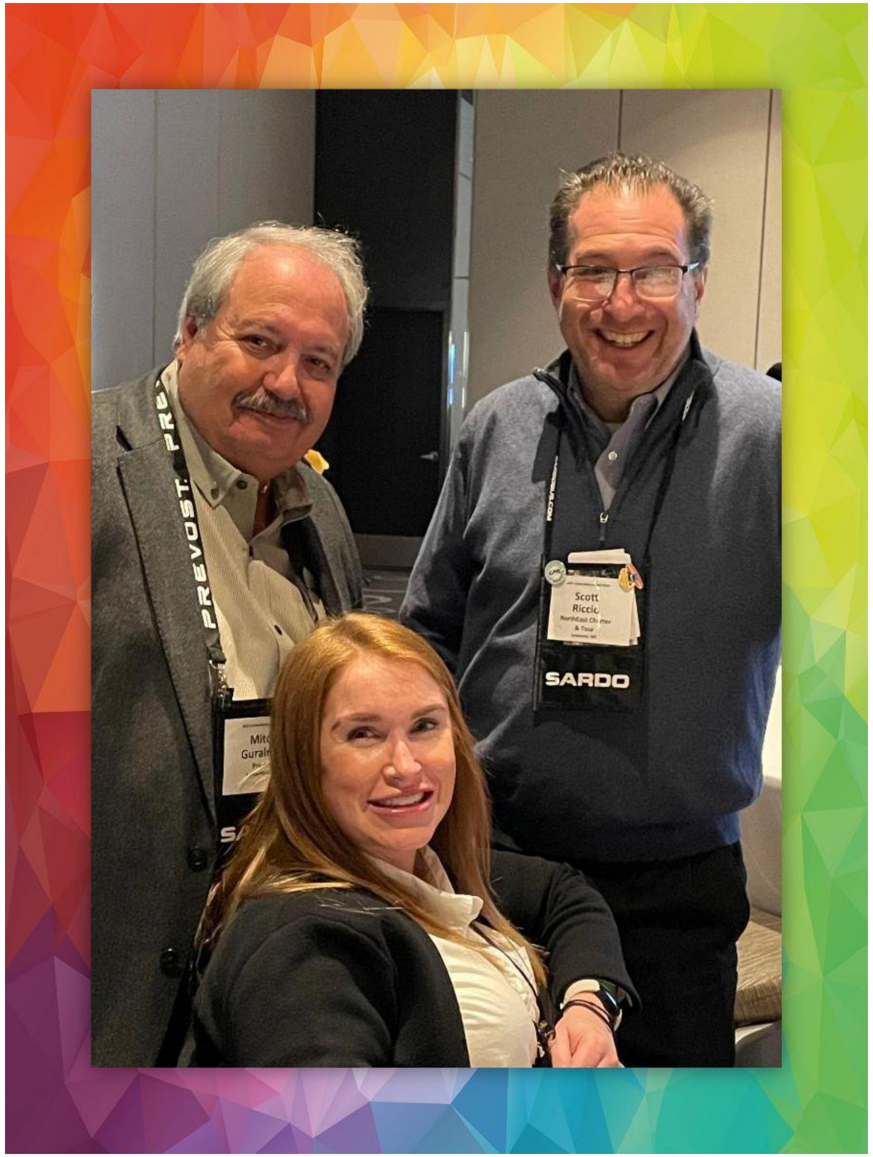
Budget TRUCK AND AUTO INC.

SAUCON™

distinctive systems™

EXPO THANK YOU

From right, EXPO CHAIR SCOTT RICCIO, UMA's Director of Meetings & Membership, Carrington Blake, and EXPO Co CHAIR, Mitch Guralnick. Plus the Committee… Thank you all!



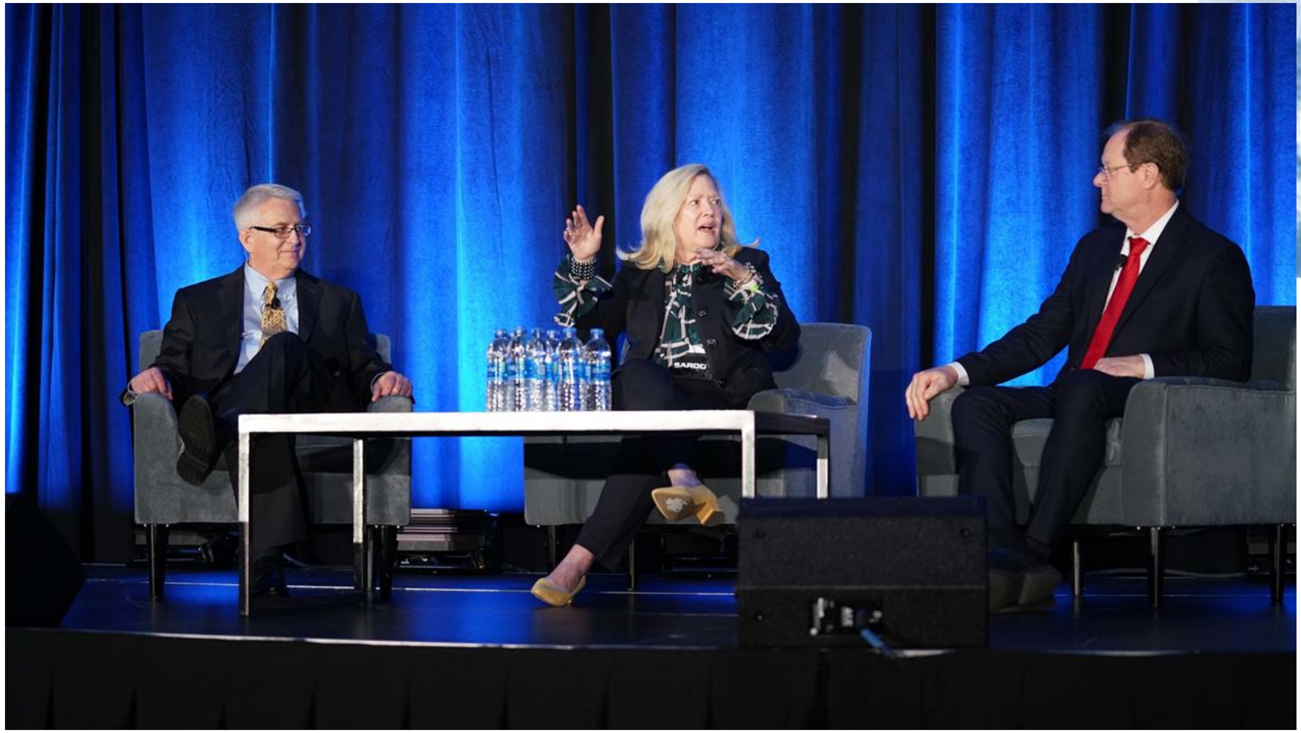
Welcome UMA Board of Directors

Board of Directors | United Motorcoach Association (uma.org)

Clarence Cox, left, at EXPO and the UMA Board of Directors meeting last Saturday in Long Beach.

Legislative & Regulatory Report

Ken Presley
Becky Weber



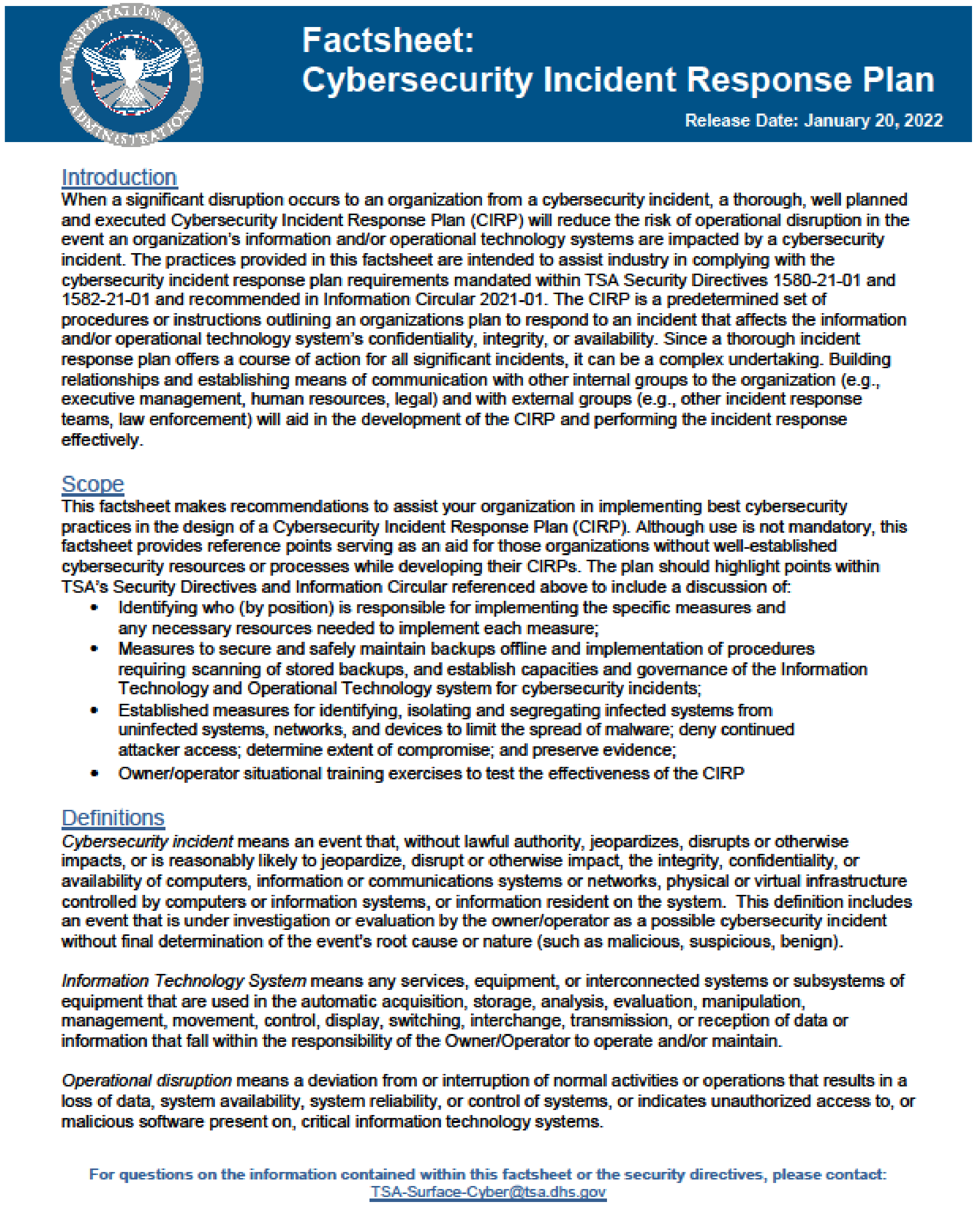
CERTS Tax Exemption

CERTS Refill ($6 billion)

TSA Update
David Cooper

David Cooper
Industry Engagement Branch Manager
Industry Engagement Manager (Highway)
Policy, Plans, and Engagement (Surface Policy Division)
Transportation Security Administration
U.S. Department of Homeland Security
Office: 571-227-2609 / Cell: 202-870-9970
David.Cooper1@tsa.dhs.gov

Incident Response Plan



Factsheet:
Cybersecurity Incident Response Plan

Release Date: January 20, 2022

Introduction

When a significant disruption occurs to an organization from a cybersecurity incident, a thorough, well planned and executed Cybersecurity Incident Response Plan (CIRP) will reduce the risk of operational disruption in the event an organization's information and/or operational technology systems are impacted by a cybersecurity incident. The practices provided in this factsheet are intended to assist industry in complying with the cybersecurity incident response plan requirements mandated within TSA Security Directives 1580-21-01 and 1582-21-01 and recommended in Information Circular 2021-01. The CIRP is a predetermined set of procedures or instructions outlining an organizations plan to respond to an incident that affects the information and/or operational technology system's confidentiality, integrity, or availability. Since a thorough incident response plan offers a course of action for all significant incidents, it can be a complex undertaking. Building relationships and establishing means of communication with other internal groups to the organization (e.g., executive management, human resources, legal) and with external groups (e.g., other incident response teams, law enforcement) will aid in the development of the CIRP and performing the incident response effectively.

Scope

This factsheet makes recommendations to assist your organization in implementing best cybersecurity practices in the design of a Cybersecurity Incident Response Plan (CIRP). Although use is not mandatory, this factsheet provides reference points serving as an aid for those organizations without well-established cybersecurity resources or processes while developing their CIRPs. The plan should highlight points within TSA's Security Directives and Information Circular referenced above to include a discussion of:

- Identifying who (by position) is responsible for implementing the specific measures and any necessary resources needed to implement each measure;
- Measures to secure and safely maintain backups offline and implementation of procedures requiring scanning of stored backups, and establish capacities and governance of the Information Technology and Operational Technology system for cybersecurity incidents;
- Established measures for identifying, isolating and segregating infected systems from uninfected systems, networks, and devices to limit the spread of malware; deny continued attacker access; determine extent of compromise; and preserve evidence;
- Owner/operator situational training exercises to test the effectiveness of the CIRP

Definitions

Cybersecurity incident means an event that, without lawful authority, jeopardizes, disrupts or otherwise impacts, or is reasonably likely to jeopardize, disrupt or otherwise impact, the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on the system. This definition includes an event that is under investigation or evaluation by the owner/operator as a possible cybersecurity incident without final determination of the event's root cause or nature (such as malicious, suspicious, benign).

Information Technology System means any services, equipment, or interconnected systems or subsystems of equipment that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information that fall within the responsibility of the Owner/Operator to operate and/or maintain.

Operational disruption means a deviation from or interruption of normal activities or operations that results in a loss of data, system availability, system reliability, or control of systems, or indicates unauthorized access to, or malicious software present on, critical information technology systems.

For questions on the information contained within this factsheet or the security directives, please contact:
TSA-Surface-Cyber@tsa.dhs.gov

Enhancing Surface Transportation Cybersecurity

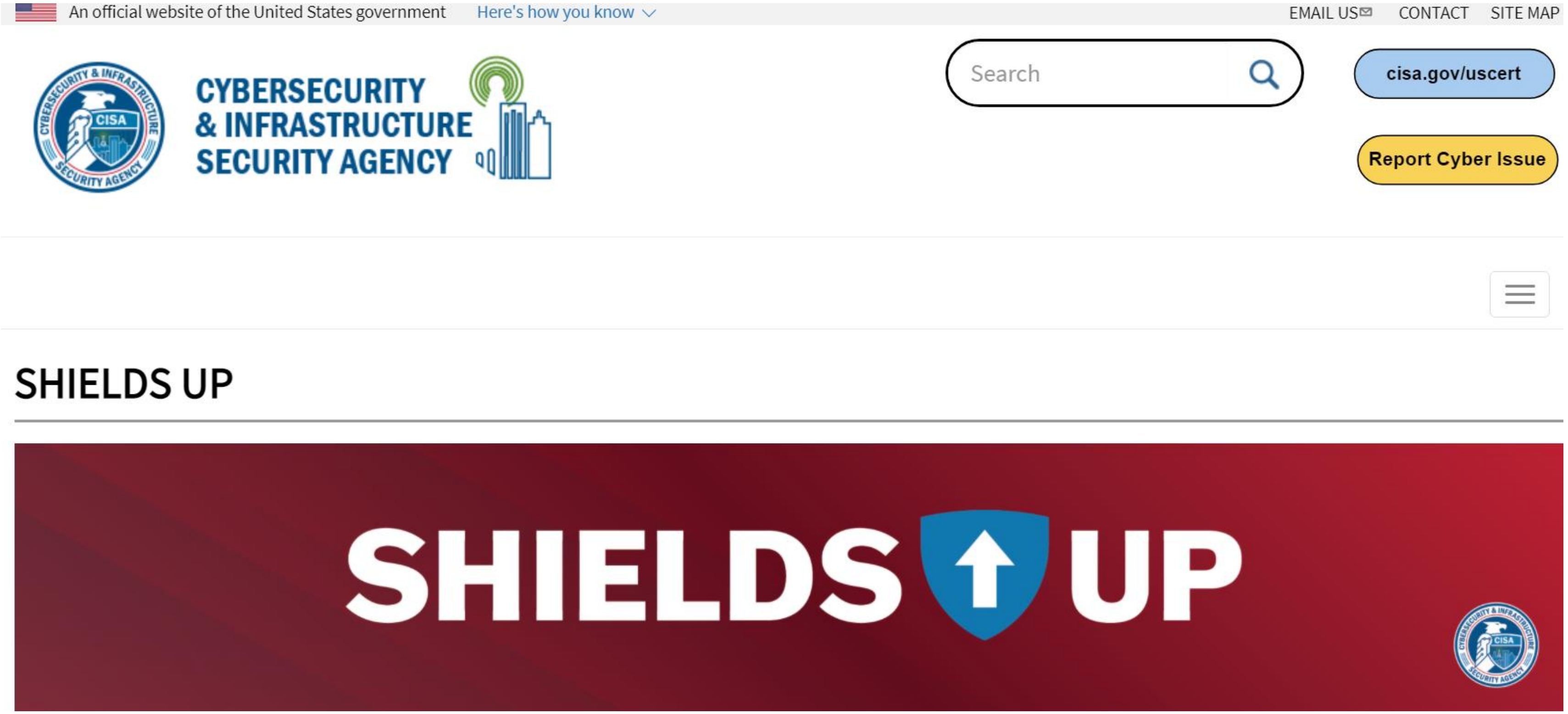
IC Surface Transportation-2022-01

EFFECTIVE DATE February 25, 2022

DHS/CISA “Shields Up”

DHS/CISA “Shields Up” site is a significant resource.

https://www.cisa.gov/shields-up

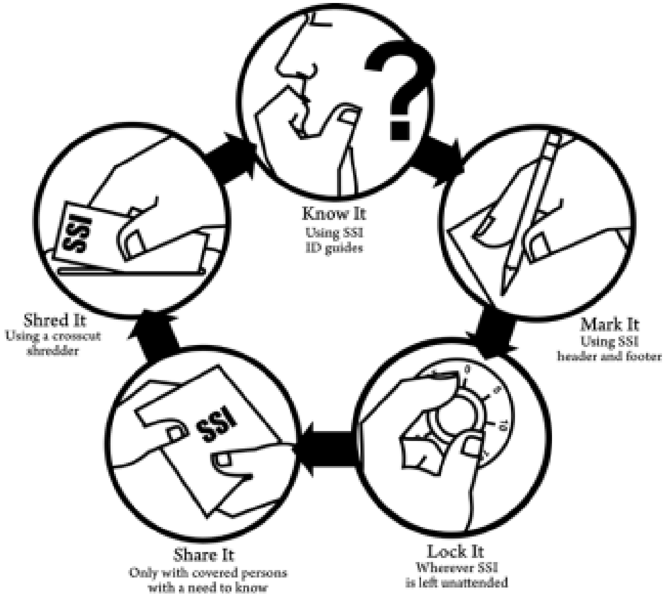


An official website of the United States government

DEPARTMENT OF HOMELAND SECURITY

SENSITIVE SECURITY INFORMATION

Cover Sheet


Know It
Using SSI ID guides
Mark It
Using SSI header and footer
Lock It
Wherever SSI is left unattended
Share It
Only with covered persons with a need to know
Shred It
Using a crosscut shredder
SSI
SSI

For more information on handling SSI, contact SSI@dhs.gov.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

Reference: 49 CFR § 1520.13, Marking SSI

Factsheet:
Cybersecurity Incident Response Plan

Release Date: January 20, 2022

Introduction

When a significant disruption occurs to an organization from a cybersecurity incident, a thorough, well planned and executed Cybersecurity Incident Response Plan (CIRP) will reduce the risk of operational disruption in the event an organization's information and/or operational technology systems are impacted by a cybersecurity incident. The practices provided in this factsheet are intended to assist industry in complying with the cybersecurity incident response plan requirements mandated within TSA Security Directives 1580-21-01 and 1582-21-01 and recommended in Information Circular 2021-01. The CIRP is a predetermined set of procedures or instructions outlining an organizations plan to respond to an incident that affects the information and/or operational technology system's confidentiality, integrity, or availability. Since a thorough incident response plan offers a course of action for all significant incidents, it can be a complex undertaking. Building relationships and establishing means of communication with other internal groups to the organization (e.g., executive management, human resources, legal) and with external groups (e.g., other incident response teams, law enforcement) will aid in the development of the CIRP and performing the incident response effectively.

SAVE THE DATES
2023 UMA EXPO
Jan. 11-14, 2023

Visit Orlando®

Imagine Orlando | Visit Orlando - YouTube