



MILE HIGH DICE

CYBERSECURITY SEMINAR & TABLETOP EXERCISE **PARTICIPANT HANDBOOK**

NOVEMBER 10, 2016



FEMA



CONTENTS

LOCATION	2
MILE HIGH DICE PLANNING TEAM	3
AGENDA	4
INTRODUCTION	5
REAL WORLD EXAMPLES OF THE TTX SCENARIOS	6
GLOSSARY	8
SPEAKER BIOS	10
CYBERSECURITY RESOURCES AND DOCTRINE	11

LOCATION

Federal Bureau of Prisons National Corrections Academy
11900 East Cornell Avenue Unit C | Vail Room | Aurora CO 80014

****IMPORTANT NOTES****

- You must have your federal photo ID or another official government issued photo ID, i.e., Driver's License, to enter the building.
- DICE starts at 8:30 sharp, so be sure to leave time for parking and going through security when you enter the building.
- Firearms are not allowed in the building (even for law enforcement), so please ensure that you make arrangements to store them prior to entering the building.
- Lunch will not be provided. There are plenty of eateries within walking distance or a short drive. The facility has a student break area room with vending machines, microwave oven and a refrigerator if you choose to bring your own lunch.



PLANNING TEAM | THANK YOU

BUREAU OF PRISONS, NATIONAL CORRECTIONS ACADEMY

- * Jim Gray, Director

COLORADO EMERGENCY PREPAREDNESS PARTNERSHIP

- * Pat Williams, Executive Director

COLORADO FEDERAL EXECUTIVE BOARD

- * Fred Eidson, Chair & DOC EDA Administrative Director
- * Gay Page, Executive Director
- * Jeff Conn, Outreach Strategist
- * Donna Vallejos, GSA & Emergency Preparedness Council Chair
- * Jackie Mead, ONRR & Emergency Preparedness Council Secretary
- * Sheila Perry, ONRR & Emergency Preparedness Council Past Chair
- * Vickie Deal, GSA

DEPARTMENT OF HOMELAND SECURITY, FEDERAL EMERGENCY MANAGEMENT AGENCY

- * Nancy Dragani, Regional Administrator (A)
- * Mike Brinkman, Continuity Program Manager
- * Mary Beth Vasco, JD, MEP, Tech Hazards Specialist

DEPARTMENT OF HOMELAND SECURITY, NATIONAL CYBER EXERCISE & PLANNING PROGRAM

- * Bill Bauer, Exercise Planner
- * Gary Benedict, Acting Chief
- * Ben Coyle, Exercise Planner
- * Jim Harris, Exercise Facilitator

DEPARTMENT OF HOMELAND SECURITY, NATIONAL PROTECTION & PROGRAMS DIRECTORATE

- * Joe O'Keefe, Protective Security Advisor
- * Jamie Richards, Protective Security Advisor
- * Harley Rinerson, Cyber Security Advisor

STATE OF COLORADO, DEPARTMENT OF HOMELAND SECURITY & EMERGENCY MANAGEMENT

- * Jory Maes, Infrastructure Protection Program Manager
- * Fran Santagata, Preparedness Program Manager

WESTERN AREA POWER ADMINISTRATION

- * Randy Dreiling, Cybersecurity
- * Tiffani DeFore, Emergency Management
- * Orlando Reyes, Operations

AGENDA

7:30 am	Registration	Participants sign in
8:30	Welcome	Opening Remarks Gay Page, CFEB Executive Director Jim Gray, BOP NCA Director Fred Eidson, CFEB Chair & DOC EDA Administrative Director Nancy Dragani, FEMA Regional Administrator (A) Introductions & COOP in 90 Seconds Mike Brinkman, FEMA Region 8 Continuity Program Manager
9:30	Scenario 1	Ransomware Facilitator James Harris, DHS
10:30	BREAK	
10:50	Scenario 2	Watering Hole Facilitator James Harris, DHS
11:50	LUNCH	On Your Own
1:10 pm	Scenario 3	Cyber-Induced Power Outage Facilitator James Harris, DHS
2:10	BREAK	
2:30	Scenario 4	Insider Threat Facilitator James Harris, DHS
3:30	Wrap Up	Mike Brinkman
3:45	Adjourn	

INTRODUCTION

BACKGROUND

The Mile High Denver Interagency Continuity Exercise (DICE) is an annual continuity exercise hosted by the Colorado Federal Executive Board (CFEB) and the Federal Emergency Management Agency (FEMA). What began as a Denver area exercise for Federal agencies now includes state government from the six states that make up FEMA Region VIII (Colorado, Montana, North Dakota, South Dakota, Utah and Wyoming) along with cities and counties. The exercise provides participants the opportunity to improve their continuity plans and procedures by learning the latest policy updates, discussing their continuity planning efforts, testing their planning assumptions, and sharing best practices.

PURPOSE

Mile High DICE provides a forum for interagency coordination and improvement of continuity and response plans. The 2016 theme is cybersecurity, which is the RISC (Regional Interagency Steering Committee) priority this year. DICE establishes a learning environment for participants to improve their understanding of a cyber incident and examine response/contingency plans to determine their ability to continue their mission essential functions.

OBJECTIVES

- Develop a common understanding of:
 - Cybersecurity threats and vulnerabilities
 - Cyber resources available from the government
- Identify cyber gaps or vulnerabilities that could disrupt delivery of mission essential functions
- Discuss response and recovery of mission essential functions following a cyber event
- Deliver sample tools that will assist in the development of a cyber annex in the organization's plan(s).

REAL WORLD EXAMPLES OF THE TTX SCENARIOS

SCENARIO 1 | RANSOMWARE

Crypto-ransomware attack encrypts entire New Jersey school district network.

<http://www.networkworld.com/article/2901527/microsoft-subnet/crypto-ransomware-attack-hit-new-jersey-school-district-locked-up-entire-network.html>

Ransomware is a type of malware program that infects, locks, or takes control of a system and demands ransom to control. Crypto-ransomware is a type of malware that encrypts files on the victim machine using strong cryptography. After that it notifies the user that their files were encrypted and demands a decryption ransom.

A New Jersey school district was hit with crypto-ransomware, requiring a federal investigation which suspended the computerized PARCC exams. Oddly, reported ransom amounts range from \$500 in bitcoins to 500 bitcoins worth about \$124,000.00.

SCENARIO 2 | WATERING HOLE

Chinese Attackers Hacked Forbes Website in Watering Hole Attack: Security Firms.

<http://www.securityweek.com/chinese-attackers-hacked-forbes-website-watering-hole-attack-security-firms>

A technique malicious actors' use in cyber espionage or theft. Hacker's motivations are to steal intellectual property, personal information, or gain access to sensitive computer systems. They do this by injecting exploits into selected sites often visited by the targeted victims. Once the selected site is identified, exploits drop malware onto the vulnerable systems through the victims' trusted sites.

According to two security companies, in November 2014, a Chinese attack group infected Forbes.com using a watering hole attack, targeting visitors working in the financial services and defense industries.

SCENARIO 3 | CYBER-INDUCED PHYSICAL CONSEQUENCES

A Cyber Attack Has Caused Confirmed Physical Damage for the Second Time Ever.

<https://www.wired.com/2015/01/german-steel-mill-hack-destruction/>

This article highlights the need for strong cybersecurity within industrial control systems. It describes the second time in history that a cyber-attack induced physical consequences. This attack specifically targeted a German steel mill and disrupted its control systems to such a degree that a blast furnace could not properly shut down, resulting in massive, although unspecified damage.

SCENARIO 4 | INSIDER THREAT

9 employee insiders who breached security.

<http://www.csoonline.com/article/2692072/data-protection/data-protection-165097-disgruntled-employees-lash-out.html>

For many, especially in recent history, insider threats are and have been associated with active shooters. While that is still a realistic threat, cyber related insider threats are becoming more and more prominent. This article provides nine brief examples of how insider threats can now be cyber related.

GLOSSARY

Bitcoin

Bitcoin is essentially cash for the internet. Bitcoin is a consensus network that enables a new payment system and a completely digital money. It is the first decentralized peer-to-peer payment network that is powered by its users with no central authority or middlemen.

Denial of Service Attack (DOS)

The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)

Distributed Denial of Service Attack (DDoS)

A Denial of Service technique that uses numerous hosts to perform the attack.

Industrial Control System (ICS)

Integrated hardware and software designed to monitor and control the operation of machinery and associated devices in industrial environments.

Internet Protocol (IP)

The method or protocol by which data is sent from one computer to another on the Internet.

Malware

A generic term for a number of different types of malicious code.

Ransomware Attack

Perpetrators use ransomware to encrypt a user's important files and documents, making them unreadable, until a ransom is paid.

Supervisory Control and Data Acquisition (SCADA)

Used to monitor and remotely control critical industrial processes, such as gas pipelines, electric power transmission and water distribution.

Watering Hole Attack

A technique malicious actors utilize in cyber espionage or theft. Hacker's motivations are to steal intellectual property, personal information or gain access to sensitive computer systems. They do this by injecting exploits into selected sites often visited by the targeted victims. Once identified, exploits drop malware onto the vulnerable systems through the victims trusted sites.

GLOSSARY RESOURCE LINKS

NISTIR 7298 Revision 2, Glossary of Key Information Security Terms

<http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>

SANS <http://www.sans.org/security-resources/glossary-of-terms>

BITCOIN <https://www.bitcoin.com/faq>

RANSOMWARE <https://www.fbi.gov/contact-us/field-offices/cleveland/news/press-releases/ransomware-latest-cyber-extortion-tool>

WATERING HOLE https://ics-cert.us-cert.gov/sites/default/files/documents/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_S508C.pdf

SPEAKER BIOS

DHS NATIONAL CYBER EXERCISE & PLANNING PROGRAM TEAM

Ben Coyle-

Ben Coyle earned his Master's Degree from George Washington University in Security and Safety Leadership. He was a White House Intern within the Executive Office of the President, has spent time as a contracted OPM Investigator, Department of Energy Cyber Security Specialist, and Cyber Exercise Planner with Aveshka supporting the National Cyber Exercise & Planning Program at the Department of Homeland Security.

Jim Harris-

Jim Harris was an Engineer/ Scientist for IBM in the mid-nineties before joining the FBI after 9/11. Jim served as a Special Agent within the Cyber Division and finished his career with the FBI as the Assistant Section Chief of Counterterrorism Internet Operations. Since 2013 Jim has been working as a consultant for public and private sector companies planning and preparing for cyber incidents and is one of the primary cyber exercise facilitators for the National Cyber Exercise & Planning Program at the Department of Homeland Security.

Bill Bauer-

Bill Bauer is a Cyber Exercise Planner with Aveshka supporting the National Cyber Exercise program within the Department of Homeland Security. Bill earned an Associate's Degree in Fire Science from the Community College of the Air Force and a Bachelor's Degree in Fire and Emergency Management from Kaplan University. Bill Bauer served over 23 years in the United States Air Force in the Fire and Emergency Services career field. Since his retirement he has provided WMD, exercise, emergency planning and Continuity of Operations support to the Department of Defense, DHS Science and Technology and DHS Office of Infrastructure Protection, Protective Security Coordination Division.

CYBERSECURITY RESOURCES AND DOCTRINE

PRINCIPAL DOCTRINE

Presidential Policy Directive 41-United States Cyber Incident Coordination

<https://www.whitehouse.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>

Comprehensive National Cybersecurity Initiative (CNCI) (2009)

<http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative>

Cyberspace Policy Review (2009)

http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

Executive Order 13636: Improving Critical Infrastructure Cybersecurity (2013)

<http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>

Framework for Improving Critical Infrastructure Cybersecurity (2014)

<http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>

Homeland Security Presidential Directive 7 (HSPD 7) (2003)

<https://www.dhs.gov/homeland-security-presidential-directive-7>

International Strategy for Cyberspace (2011)

https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

National Infrastructure Protection Plan (NIPP) 2013

<http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience>

National Institute of Standards and Technology Computer Security Incident Handling Guide (2012)

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

National Institute of Standards and Technology: Framework for Improving Critical Infrastructure Cybersecurity (2014)

<http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>

National Response Framework (2013)

http://www.fema.gov/media-library-data/20130726-1914-25045-1246/final_national_response_framework_20130501.pdf

National Strategy for Trusted Identities in Cyberspace (2011)

http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (2013)

<http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>

DEPARTMENT OF HOMELAND SECURITY

Cyber Capabilities/Entities

- National Cybersecurity and Communications Integration Center (NCCIC) (contact: NCCIC@hq.dhs.gov; 888-282-0870)
 - Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (contact: ics-cert@hq.dhs.gov)
 - National Coordinating Center for Communications (NCC) (contact: NCC@hq.dhs.gov)
 - United States Computer Emergency Readiness Team (US-CERT) (contact: info@us-cert.gov)
- National Infrastructure Coordinating Center (contact: NICC@hq.dhs.gov)

Resources/Documents

Informing Cyber Storm V: Lessons Learned from Cyber Storm IV (2015)

<https://www.dhs.gov/sites/default/files/publications/Lessons%20Learned%20from%20Cyber%20Storm%20IV.pdf>

DHS Blueprint for a Secure Cyber Future (2011)

<http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf>

DHS Memorandum of Agreement with Department of Defense (2010)

<http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf>

The 2014 Quadrennial Homeland Security Review (2014)

<https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf>

DHS Strategic Plan Fiscal Years 2014-2018

<https://www.dhs.gov/sites/default/files/publications/FY14-18%20Strategic%20Plan.PDF>

Enabling Distributed Security in Cyberspace (2011)

<http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf>

ICS-CERT Monitor: Incident Response Activity September 2014-February 2015

https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf

ICS-CERT Fact Sheet (2016)

https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_ICSCERT_S508C.pdf

Protected Critical Infrastructure Information (PCII) Program Fact Sheet (2015)

<https://www.dhs.gov/protected-critical-infrastructure-information-pcii-program>

Written testimony of U.S. Department of Homeland Security, National Protection and Programs Directorate, Office of Cybersecurity & Communications Assistant Secretary Dr. Andy Ozment for a House Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, hearing titled “DHS’ Effort to Secure .Gov” Cybersecurity Mission: Promoting Innovation and Securing Critical Infrastructure”

<https://www.dhs.gov/news/2015/06/24/written-testimony-nppd-house-homeland-security-subcommittee-cybersecurity>

Written testimony of Department of Homeland Security Secretary Jeh Johnson for a Senate Committee on Homeland Security and Governmental Affairs hearing titled “Threats to the Homeland”

<https://www.dhs.gov/news/2015/10/08/written-testimony-dhs-secretary-jeh-johnson-senate-committee-homeland-security-and>

STATE GOVERNMENT

Cyber Capabilities/Entities

Multi-State Information Sharing and Analysis Center (MS-ISAC) (contact: info@msisac.org; 518-266-3460)

Resources/Documents

Cybersecurity and the States (National Association of State Chief Information Officers [NASCIO])

<http://www.nascio.org/Advocacy/Cybersecurity>

MS-ISAC Charter (2013)

<https://msisac.cisecurity.org/about/charter/documents/MS-ISACCharter2013-03.pdf>

MS-ISAC Cyber Incident Response Guide: A Non-Technical Guide

<http://msisac.cisecurity.org/members/localgovernment/documents/FINALIncidentResponseGuide.pdf>

NGA Resource Center

<http://www.nga.org/cms/statecyber>

PRIVATE SECTOR/BUSINESS

Cyber Capabilities/Entities

Business Executives for National Security <http://www.bens.org/>

Electronic Privacy Information Center <http://epic.org/>

Information Sharing and Analysis Centers (ISACs)

Internet Security Alliance <http://www.isalliance.org/>

National Council of ISACs <http://www.isaccouncil.org/>

Partnership for Critical Infrastructure Security <http://www.sheriffs.org/content/partnership-critical-infrastructure-security>

Resources/Documents

Commonsense Guide to Cyber Security for Small Businesses (U.S. Chamber of Commerce) (2004)

<https://www.uschamber.com/sites/default/files/legacy/reports/cybersecurityguide923.pdf>

ISAlliance/ANSI Report: The Financial Management of Cyber Risk (2010)

<http://www.ndia.org/Divisions/Divisions/Cyber/Documents/ISAlliance.pdf>

The Role of the ISACs in Critical Infrastructure Resilience (2014)

http://www.rsaconference.com/writable/presentations/file_upload/cle-t10-the-role-of-the-isacs-in-critical-infrastructure-resilience.pdf

Verizon Data Breaches Investigations Report (2016)

<http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/>

Critical Infrastructure Cyber Community Voluntary Program

<https://www.us-cert.gov/ccubedvp>

TRAINING RESOURCE LINKS

Cybersecurity Training and Exercises

<https://www.dhs.gov/cybersecurity-training-exercises>

Texas A&M Engineering Extension Service (TEEX)

<https://teex.org/Pages/homeland-security.aspx>

MISC. RESOURCES

Multi-State Information Sharing and Analysis Center Cyber Incident Response Guide

<https://msisac.cisecurity.org/>

A non-technical guide for business managers, office managers and operations managers designed for small businesses and agencies to further knowledge and awareness regarding cyber security.

NIST Special Publication 800-61 Revision 2 – Computer Security Incident Handling Guide

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

This publication provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident.

Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability

https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/final-RP_ics_cybersecurity_incident_response_100609.pdf

This document will present recommendations to help facilities that use control systems better prepare for and respond to a cyber incident regardless of the source.

NIST Framework for Improving Critical Infrastructure Cybersecurity

<https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>

The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes.

NIST Guide to Cyber Threat Information Sharing

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf>

Cyber threat information is any information that can help an organization identify, assess, monitor, and respond to cyber threats. This publication provides guidelines for establishing and participating in cyber threat information sharing relationships. This guidance helps organizations establish information sharing goals, identify cyber threat information sources, scope information sharing activities, develop rules that control the publication and distribution of threat information, engage with existing sharing communities, and make effective use of threat information in support of the organization's overall cybersecurity practices.

Law Enforcement Cyber Incident Reporting – A Unified Message for State, Local, Tribal, and Territorial Law Enforcement

<https://www.dhs.gov/sites/default/files/publications/Law%20Enforcement%20Cyber%20Incident%20Reporting.pdf>

This document details different ways State, Local, Tribal, and Territorial law enforcement partners can report suspected or confirmed cyber incidents to the federal government.

US-CERT (United States Computer Emergency Readiness Team)

<https://www.us-cert.gov/ccubedvp/assessments>

PARTICIPANT FEEDBACK FORM

Thank you for participating in this exercise. Your observations, comments, and input are greatly appreciated, and provide invaluable insight that will better prepare our nation against threats and hazards. Any comments provided will be treated in a sensitive manner and all personal information will remain confidential. Please keep comments concise, specific, and constructive.

Part I: General Information

Please enter your responses in the form field or check box after the appropriate selection.

Name (OPTIONAL): _____

Agency/Organization Affiliation (OPTIONAL): _____

Position Title (OPTIONAL): _____

Years of Experience in Present Position: _____

Number of Exercises Previously Participated in: 0 1-5 5-10 15+

Exercise Role: Player Facilitator/Controller Observer Evaluator

Part II: Exercise Design

Please rate, on a scale of 1 to 5, your overall assessment of the exercise relative to the statements provided, with 1 indicating strong disagreement and 5 indicating strong agreement.

Assessment Factor	Strongly Disagree					Strongly Agree
Pre-exercise briefings were informative and provided the necessary information for my role in the exercise.	1	2	3	4	5	
The exercise scenario was plausible and realistic.	1	2	3	4	5	
Exercise participants included the right people in terms of level and mix of disciplines.	1	2	3	4	5	
The exercise increased my awareness to gather and analyze threat and vulnerability information.	1	2	3	4	5	
The exercise participation was appropriate for someone in my field with my level of experience/training.	1	2	3	4	5	
Comments:						
Exercise Objectives						
Develop a common understanding of: -Cybersecurity threats and vulnerabilities	1	2	3	4	5	
-Cyber resources available from the government.	1	2	3	4	5	

**Mile High DICE
Cybersecurity Seminar and
Tabletop Exercise**

Identify cyber gaps or vulnerabilities that could disrupt delivery of mission essential functions.	1	2	3	4	5
Discuss response and recovery of mission essential functions following a cyber event.	1	2	3	4	5
Deliver sample tools that will assist in the development of a cyber annex in the organization's plan(s).	1	2	3	4	5

Please identify one private, public, or non-profit organization that was *not present* for the exercise but could have benefited or provided valuable input.

Part III: Participant Feedback

1. I observed the following two (2) strengths and two (2) areas for improvement during this exercise:

Strengths	
1	
2	

Areas for Improvement	
1	
2	

2. Which exercise materials were most useful? Please identify any additional materials or resources that would be useful.

3. Please provide any recommendations on how this exercise or future exercises could be improved or enhanced.
