Participant Handbook

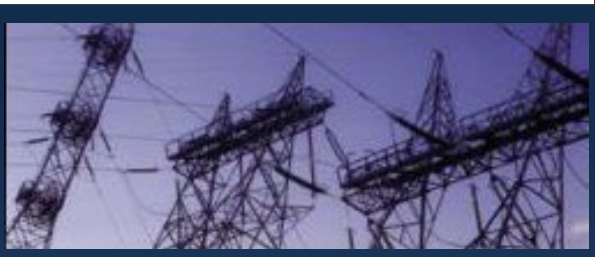
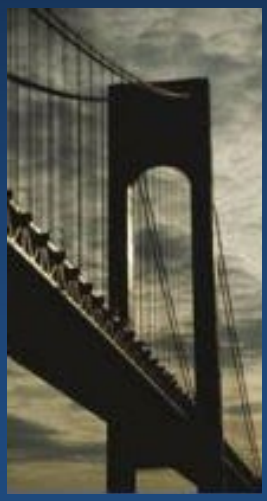
MILE HIGH DICE
Seminar

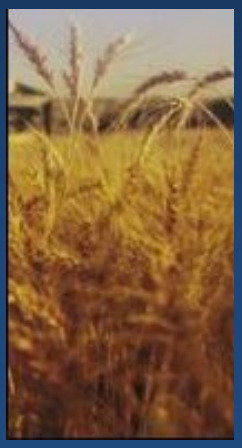
NOVEMBER 9, 2022

Existential Threats and America's Critical Infrastructure

Exploring the interface between physical and cyber threats, vulnerabilities, and solutions






FEDERAL EXECUTIVE BOARD COLORADO

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

U.S. DEPARTMENT OF HOMELAND SECURITY FEMA

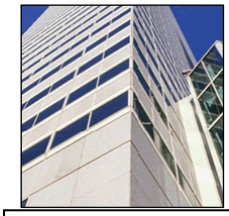
FOR OFFICIAL USE ONLY

What Comprises America's Critical Infrastructure……

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. *This directive supersedes Homeland Security Presidential Directive 7.*

Communications Sector

Chemical Sector



Commercial Facilities Sector

Critical Manufacturing Sector

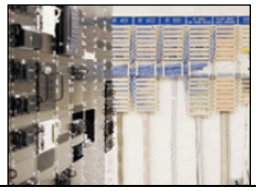
Dams Sector

Government Facilities Sector

Healthcare and Public Health Sector

Defense Industrial Base Sector

Emergency Services Sector



Information Technology Sector

Nuclear Reactors, Materials, and Waste Sector

Energy Sector

Financial Services Sector

Transportation Sector

Water and Wastewater Systems Sector

Food and Agriculture Sector

CONTENTS

MILE HIGH DICE
SEMINAR AGENDA

Time (MST)	Session	Comments
7:30 am	Registration	
8:00 am	Welcome	Opening comments • Fred Eidson, *Executive Director, Colorado Federal Executive Board (CFEB)* • Mike Harris, Deputy *Director, Bureau of Prisons-National Corrections Academy* • Nancy J. Dragani, *Regional Administrator, FEMA Region VIII* • Shawn Graff, *Regional Director, DHS/Cybersecurity and Infrastructure Security Agency (CISA)*
8:30 am	Training #1 Understanding climate change effects on critical infrastructure	Sunny Wescott *Lead Meteorologist – Collaboration Cell* *Infrastructure Security Division (ISD)* *Cybersecurity and Infrastructure Security Agency (CISA)* Learning Objectives: 1. Climate Trends of Concern Across the Nation and Forecasted Atmospheric Shifts 2. Critical Infrastructure, Supply Chain, and Stakeholder Impacts from Weather Events 3. Effective Climate Resiliency Best Practices – National and State Specific
9:30 am	Break	
9:45 am	Training #2 Interface between physical and cyber threats	V. Susan Peediyakkal *Office of the Chief Information Officer (OCIO)* *National Aeronautics and Space Administration (NASA)*
10:45 am	Break	
11:00 am	Training #3 Space Weather and Electromagnetic Pulse (EMP) threats	William (Bill) Murtagh *Program Coordinator* *Space Weather Prediction Center (SWPC)* *National Oceanic and Atmospheric Administration (NOAA)*
12:00 pm	Lunch	On your own
1:00 pm	Training #4 Panel Discussion	Q and A with Subject Matter Experts
2:15 pm	Break	
2:30 pm	Salute to Veterans: Operation Eagle Claw	Glen 'Nick' Nickel *Command Sergeant Major (CSM) (R)* *United States Army*
3:15 pm	Hot wash/final comments	
3:30 pm	Adjourn	

INTRODUCTION

Background

Mile High Dice is a recurring training event, this year sponsored by the Colorado Federal Executive Board (CFEB), the Cybersecurity and Infrastructure Security Agency (CISA) Region 8, and the Federal Emergency Management Agency (FEMA) Region 8. The event provides participants the opportunity to improve their plans and procedures by learning the latest policy updates, discussing their response and contingency planning efforts, testing their planning assumptions, and sharing best practices.

Purpose and Objectives

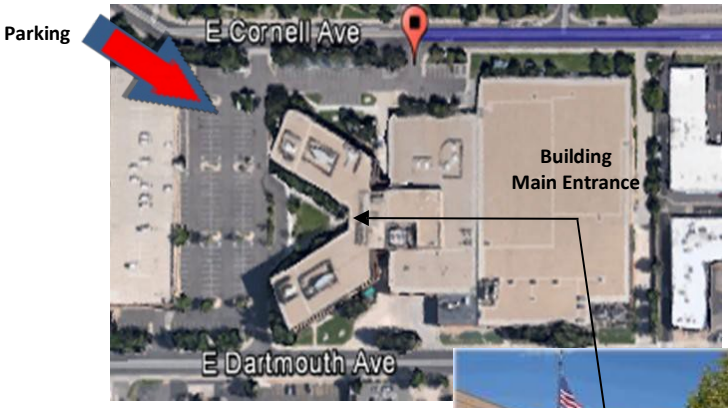
The 2022 theme is Existential Threats and America's Critical Infrastructure (Lessons Learned, Future Risks, Organizational Concerns, Individual Questions). Today's objectives include:

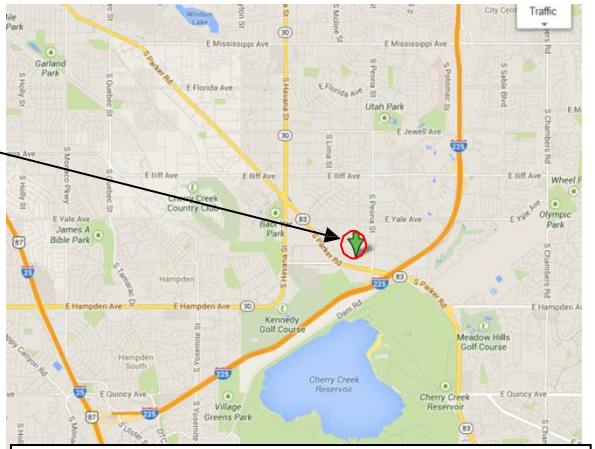
- Develop a common understanding of:
  - The existential threats to the nation's Critical Infrastructure and how can we address some of the common vulnerabilities
  - The interface between physical and cyber threats, (information technology and operational technology)
- Facilitate active learning opportunities and peer-to-peer exchanges.
- Honor those who have served our nation by learning more about the individuals who wore the uniform.
- Discuss and examine the challenges, issues and cascading impacts associated with conducting essential functions if your primary staff are affected.

Facility Overview

The event will be held in the Vail room at the Bureau of Prisons National Corrections Academy.
Note: The top level of the parking garage is restricted to GSA vehicles.

BOP National Corrections Academy
11900 East Cornell Avenue
Aurora, Colorado





DIRECTIONS FROM I 225 & PARKER RD
North on Parker Road
North (Right) on South Peoria St West (Left) on East Cornell Ave Left into the parking lot for UNIT C
The training academy is in an office complex – you will see their National Corrections Academy sign as you enter the parking lot.
IMPORTANT NOTE
You must have your Government (federal, state or local) employment photo ID or another official government issued photo ID, i.e., Driver's License, to enter the building.

***Facility fire arm policy for Law Enforcement:** Only responding (not visiting / meeting / student / attending) law enforcement are allowed to enter with weapons. There is no visitor weapons locker on site, if authorized to carry a weapon, you must secure it IAW governing policy.

This page is intentionally left blank.

What is an existential threat?

An existential threat is a threat to something's very existence—when the continued being of something is at stake or in danger. It is used to describe threats to actual living things as well to nonliving things, such as a country or an ideology[1].

Where does existential threat come from?

Something is generally considered an *existential threat* when it is massive in scale, such as climate change or nuclear warfare. The phrase *existential threat* gets used when the continued existence of something is perceived to be at stake due to some force or action.

The phrase *existential threat* begins to spread around the 1960–80s, perhaps due to the *existential threat* posed by nuclear weapons during the Cold War. Existential threat is used expansively in the early 2000s. Discussion of the attacks of September 11th (2001) framed terrorism as an existential threat to the West.

In 2019, the phrase *existential threat* became increasingly common in consideration of climate change, often discussed as an *existential threat* to human civilization and the environment.

Climate Change as an Existential Threat

Climate change is one of the most complex issues facing us today. It involves many dimensions – science, economics, society, politics, and moral and ethical questions – and is a global problem, felt on local scales, that will be around for thousands of years. Carbon dioxide, the heat-trapping greenhouse gas that is the primary driver of recent global warming, lingers in the atmosphere for many thousands of years, and the planet (especially the ocean) takes a while to respond to warming. So even if we stopped emitting all greenhouse gases today, global warming and climate change will continue to affect future generations. In this way, humanity is "committed" to some level of climate change[2].

Responding to climate change involves a two-pronged approach:

1. Reducing emissions of and stabilizing the levels of heat-trapping greenhouse gases in the atmosphere ("mitigation");
2. Adapting to the climate change already in the pipeline ("adaptation").

Mitigation – reducing climate change – involves reducing the flow of heat-trapping greenhouse gases into the atmosphere, either by reducing sources of these gases (for example, the burning of fossil fuels for electricity, heat, or transport) or enhancing the "sinks" that accumulate and store these gases (such as the oceans, forests, and soil). The goal of mitigation is to avoid significant human interference with Earth's climate, "stabilize greenhouse gas levels in a timeframe sufficient to allow ecosystems to adapt naturally to climate change, ensure that food production is not threatened, and to enable economic development to proceed in a sustainable manner" (from the 2014 report on Mitigation of Climate Change from the United Nations Intergovernmental Panel on Climate Change, page 4).

Adaptation – adapting to life in a changing climate – involves adjusting to actual or expected future climate. The goal is to reduce our risks from the harmful effects of climate change (like sea-level rise, more intense extreme weather events, or food insecurity). It also includes making the most of any potential beneficial opportunities associated with climate change (for example, longer growing seasons or increased yields in some regions).

Throughout history, people and societies have adjusted to and coped with changes in climate and extremes with varying degrees of success. Climate change (drought in particular) has been at least partly responsible for the rise and fall of civilizations. Earth's climate has been relatively stable for the past 10,000 years, and this stability has allowed for the development of our modern civilization and agriculture.

[1] https://www.dictionary.com
[2] https://climate.nasa.gov/solutions/adaptation-mitigation/

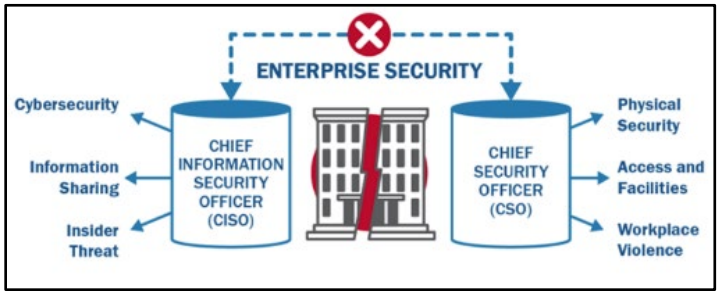
Our modern life is tailored to that stable climate and not the much warmer climate of the next thousand-plus years. As our climate changes, we will need to adapt. The faster the climate changes, the more difficult it will be.

While climate change is a global issue, it is felt on a local scale. Local governments are therefore at the frontline of adaptation. Cities and local communities around the world have been focusing on solving their own climate problems. They are working to build flood defenses, plan for heat waves and higher temperatures, install better-draining pavements to deal with floods and stormwater, and improve water storage and use.

America's infrastructure resiliency as an Existential Threat

Today's threats are a result of hybrid attacks targeting both physical and cyber assets. The adoption and integration of Internet of Things (IoT) and Industrial Internet of Things (IIoT) devices have led to an increasingly interconnected mesh of cyber-physical systems (CPS), which expands the attack surface and blurs the once clear functions of cybersecurity and physical security. Meanwhile, efforts to build cyber resilience and accelerate the adoption of advanced technologies can also introduce or exacerbate security risks in this evolving threat landscape[3].

Modern organizations grapple with two worlds. There is the traditional physical world composed of machines, electromechanical devices, manufacturing systems and other industrial equipment. Then there is the more recent digital world using servers, storage, networking and other devices used to run applications and process data. These two worlds have largely occupied separate domains, shared little (if any) meaningful data or control, and relied on oversight from business staff with distinctly different skill sets.



What is the IT/OT convergence, and how does it affect my organization in performing essential functions?

IT/OT convergence is the integration of information technology (IT) systems with operational technology (OT) systems. IT systems are used for data-centric computing; OT systems monitor events, processes, and devices, and make adjustments in enterprise and industrial operations.

Today, the worlds of IT and OT are converging. Advances in technologies are systematically allowing the digital information world to see, understand and influence the physical operational world. When implemented properly, IT/OT convergence can merge business processes, insights, and controls into a single uniform environment.

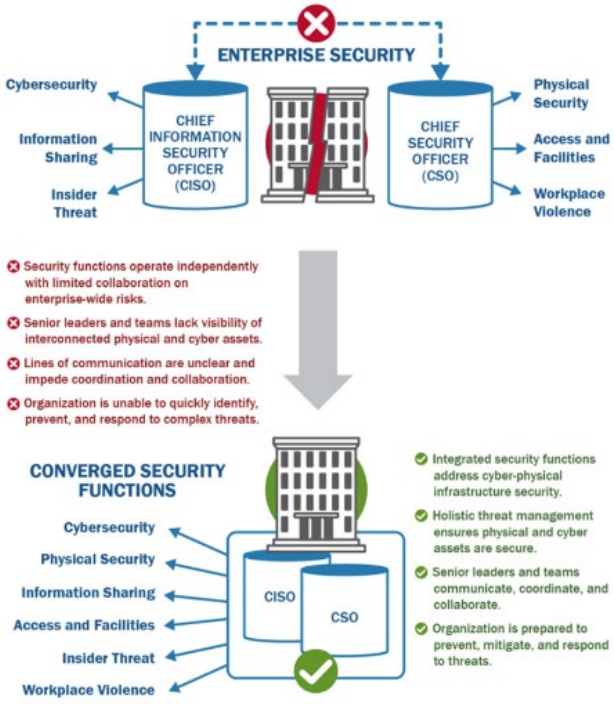
Concerns – The convergence of operating technology (OT) and information technology (IT) has a significant impact on industrial cybersecurity. In particular, industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems, which were historically physically separate, are now connected to IT systems and, therefore, the Internet. The lack of physical separation makes these systems vulnerable to a growing number of advanced threats, making them targets for hackers, spies, and cyber-warriors.

The adoption and integration of Internet of Things (IoT) and Industrial Internet of Things (IIoT) devices has led to an increasingly interconnected mesh of cyber-physical systems (CPS), which expands the attack surface and blurs the once clear functions of cybersecurity and physical security. A successful cyber or physical attack on industrial control systems and networks can disrupt operations or even deny critical services to society.

[3] https://www.cisa.gov

A successful cyber or physical attack on connected industrial control systems (ICS) and networks can disrupt operations or even deny critical services to society. For example:

- A security gap in access controls, such as unauthorized access to facilities or system permissions, can allow an individual to use a universal serial bus (USB) device or other removable hardware to introduce a virus or malware into a network.
- Heating, ventilation, and air conditioning (HVAC) systems can be virtually overridden, causing a rise in temperature that renders network servers inoperable.
- A cyber-attack on telecommunications can impair communication with law enforcement and emergency services, resulting in delayed response times.
- An unmanned aircraft system (UAS) can compromise sensitive information by gaining access to an unsecured network using wireless hacking technology.
- A cyber-attack exploiting healthcare vulnerabilities can compromise sensitive data or cause a connected medical device to malfunction, resulting in injury or loss of life.



Mitigation - converged security functions - Convergence is formal collaboration between previously disjointed security functions. Organizations with converged cybersecurity and physical security functions are more resilient and better prepared to identify, prevent, mitigate, and respond to threats. Convergence also encourages information sharing and developing unified security policies across security divisions.

What critical actions should I take back to the office?

The following are critical actions that managers and employees should be taking at this time, based upon the Continuity Preparedness Guide, CISA Shields Up recommendations, individual preparedness actions outlined on Ready.gov, and other FEMA preparedness resources.

Plans and Procedures:	
1	Validate that contact rosters and communications plans have accurate contact information for critical primary and alternate personnel and work sites using primary and back-up and alternative modes of communications.
2	Resolve any incomplete or outdated orders of succession and delegations of authority, and integrate out-of-area and devolution counterparts into daily operations to ensure seamless and continued execution of authorities and responsibilities.
3	Validate risk mitigation capabilities are in place/available to address vulnerabilities from cyber impacts identified in the Business Impact Analysis.
Personnel and Organization Capability Actions:	
4	Maintain accountability of organizational leadership and key personnel and confirm current orders of succession and delegations of authority are in place.
5	Validate individuals have family preparedness plans and go kits based upon organizational and Ready.gov guidance.
Sites, Systems, and Equipment Capability Actions:	
6	Complete CISA "Shields Up" Recommended Actions.
7	Validate primary and alternate sites' back-up power systems and supplemental fuel contracts are operational and executable for the duration of disruption to operating conditions as established in the site plans and policy requirements.
8	Conduct system tests of back-up and alternate communications systems, networks, data storage sites, and other solutions with operational partners to validate interoperability and readiness.
9	Validate communications capabilities through operational testing with senior leadership, management, and essential personnel with assigned equipment, to include, assigned secure mobile telephones, satellite communications, Priority Telecommunications Services (Government Emergency Telecommunications Service [GETS] and Wireless Priority Service [WPS]), and High Frequency (HF) radio.
10	Validate Information Technology (IT) systems are up-to-date with all required software and patches and accounted for through an inventory crosswalk to understand interconnectivity, dependencies, and restoration prioritization. The objective of this task is to ensure minimum downtime in the event of a disruption to operating conditions and the ability to sustain performance of your essential function(s) and mission critical duties.

Featured Speakers Biography

Sunny Wescott
Lead Meteorologist – Collaboration Cell
Infrastructure Security Division (ISD)
Cybersecurity and Infrastructure Security Agency (CISA)

Sunny Wescott is a Lead Meteorologist specializing in national extreme weather hazards and climatological studies for impacts to public and private sector key resources. Her previous roles working with emergency response operations for Telecommunications and Critical Infrastructure integrated her background with mission support forecasting from her previous years in the US Air Force where she trained on continental and oceanic weather as the Top Forecaster for her support region. Ms. Wescott is considered a subject matter expert for multiple climatological events such as drought, subsidence, wildfires, tropical cyclones, and extreme winter weather events.

Previously, Ms. Wescott graduated top of her class for her degrees in Homeland Security Management, Public Safety Administration, and Atmospheric Sciences prior to accepting membership with the American Meteorological Society (AMS).In addition to her degrees, Ms. Wescott holds over 60 certifications from the Federal Emergency Management Agency, the University of Colorado's COMET Meteorological Education Program, the Department of Defense Weather Technology Course, Texas A&M, the National Oceanic and Atmospheric Administration HURREVAC program, and countless certifications from the National Weather Service Subject Matter Expertise Courses.

In 2018 Ms. Wescott began supporting the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) providing support to various working groups to include the Resilient Power Working Group, CISA's Extreme Weather Working Group, the Wildfire and Drought Working Group, the National Disaster Resiliency Council, the National Risk Management Center's Climate Focus Group, and the National Water Sector Threat Team in addition to providing a weekly national-international climate summary to various partners across the nation. Her current role is providing Extreme Weather Outreach for CISA's Infrastructure Security Division (ISD) Collaboration Cell where she creates and presents briefings for regions and critical infrastructure operators using focused reports and outlooks for degradations from climate shifts.

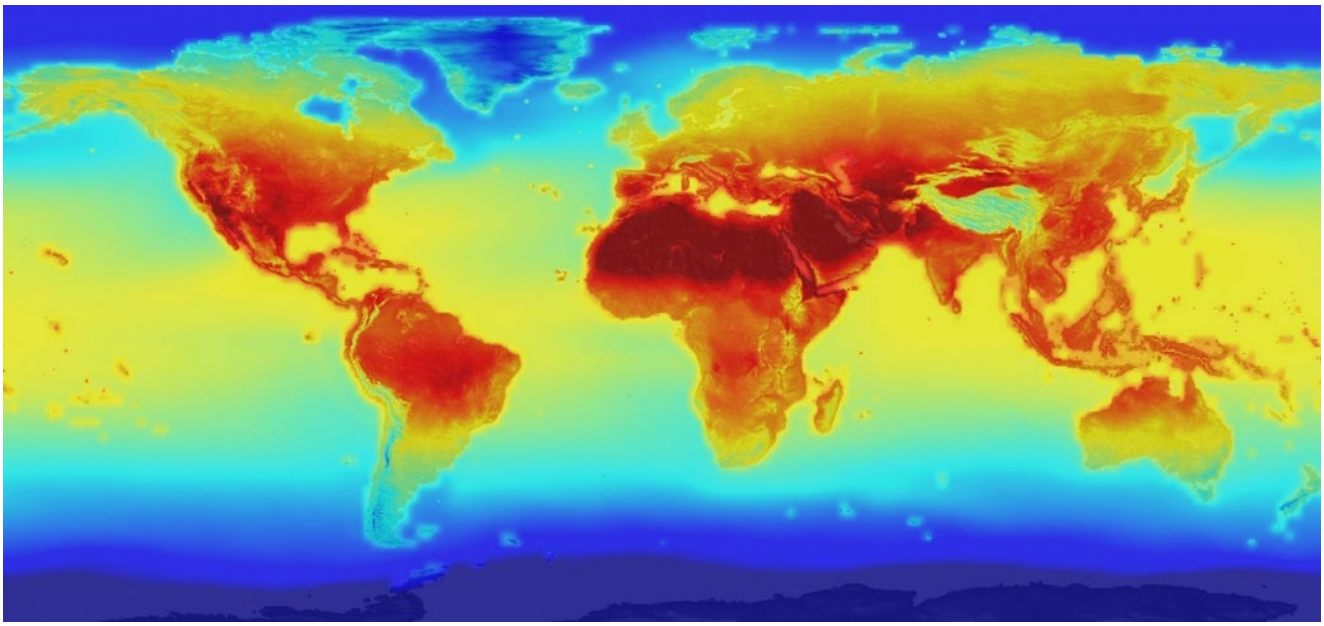
V. Susan Peediyakkal
Office of the Chief Information Officer (OCIO)
NASA Office of the Chief Information Officer
National Aeronautics and Space Administration (NASA)

NASA Office of the Chief Information Officer

With over 18 years of IT and cybersecurity experience, focused primarily on Cyber Threat Intelligence (CTI), V. Susan Peediyakkal draws on her significant knowledge from working with various intelligence operations in the federal government and international commercial domains. Susan's career began in the US Air Force where she has served 20 years, both active and reserve, before retiring in 2021. She joined NASA in October 2020 as the InfoSec Operations Manager for Ames research Center and recently transitioned to her new role as Service Management Practice Lead for the Cybersecurity Services (CyS) Service Line based out of Headquarters in DC.

An active member of the cybersecurity community; Susan is the founder and director of BSides Sacramento, serves on the board for Mental Health Hackers as the Chief Wellness Officer, and an ambassador for the Women's Society of Cyberjutsu. In February 2020, she completed her CISO certification and took “Best in CoHort” at Carnegie Mellon University. Susan was named a 2020-2022 technologist fellow for the National Security Institute (NSI) at George Mason University and appointed to the advisory board for CSU Chico's Executive Program.

In March 2018, Susan was named one of “10 Women in Security You May Not Know But Should” by one of the most widely-read cyber security news sites on the Web, Dark Reading.



William (Bill) Murtagh
Program Coordinator

National Weather Service
Space Weather Prediction Center

National Weather Service
National Oceanic and Atmospheric Administration (NOAA)

Bill Murtagh currently serves as the Program Coordinator for the National Oceanic and Atmospheric Administration (NOAA) Space Weather Prediction Center (SWPC) in Boulder, Colorado. Bill is NOAA's space weather lead in coordinating preparedness and response efforts with industry, emergency managers, and government agencies around the world. Bill also serves as the National Weather Service lead in the White House Office and Science Technology Policy (OSTP) interagency committee to develop and implement actions in the National Space Weather Strategy and Action Plan (NSWSAP).

In October 2016, he completed a 26-month assignment in OSTP as the Assistant Director for Space Weather. In his position at OSTP he oversaw the development and implementation of the 2015 National Space Weather Strategy and Action Plan and coordinated efforts to develop Executive Order 13744 (2016) – "Coordinating Efforts to Prepare the Nation for Space Weather Events".

He regularly briefs the White House, Congress, and other government leadership on space weather and the vulnerabilities of critical infrastructure to space weather storms. In October 2019, he testified in the House of Representatives in a hearing of the Joint Subcommittees on Space and Aeronautics and the Subcommittee on Environment on Space Weather: Advancing Research, Monitoring, and Forecasting Capabilities.

In February 2020, he testified in the Senate Committee on Commerce, Science, and Transportation hearing entitled Missions of National Importance: Planetary Defense, Space Weather and Space Situational Awareness. Bill is also a key contributor in U.S. government efforts to advance international cooperation in space weather-related activities. He is a regular guest speaker at universities and national and international conferences. He has provided numerous interviews to major media outlets and is featured in several documentaries on space weather.

Before joining NOAA, Bill was a weather forecaster in the United States Air Force. He coordinated and provided meteorological support for national security interests around the world. Bill transferred to the SWPC in 1997 as a USAF space weather forecaster and liaison between NOAA and the U.S. Air Force. He joined NOAA in 2003 after retiring from the Air Force with 23 years of military service.

Mr. Glen 'Nick' Nickel
Command Sergeant Major (CSM) (Retired)
United States Army

Glen "Nick Nickel retired as the Deputy Director of Operations at Special Operations Command-North (SOCNORTH). SOCNORTH is the Theater Special Operations Command (TSOC) for US Northern Command. He served there 2013 to 2020, where he worked to mitigate potential terrorist threats in North America. He was a key developer the bilateral Counterterrorism Combined Defense Plan between the U.S. and Canada, and helped establish an enduring relationship with the FBI National Mission organizations.

Mr. Nickel previously was assigned to USNORTHCOM, as the Operations Officer for the Antiterrorism/Force Protection Division. He subsequently, became the Deputy for the USNORTHCOM J32 Special Operations Division in April 2004-September 2013.

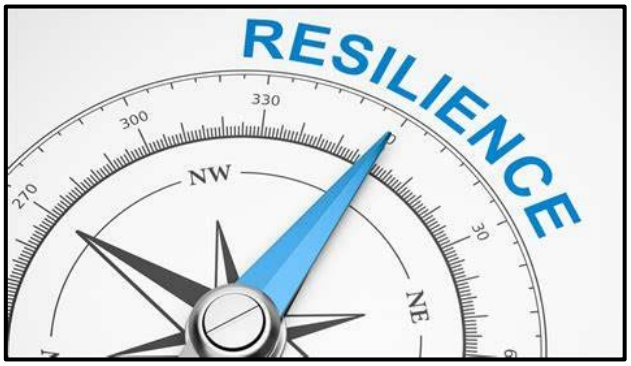
Prior to assignment at USNORTHCOM, he spent four years in the civilian sector specializing in security and disaster preparedness programs. He conducted vulnerability assessments of metropolitan water and wastewater systems) to deter terrorist attacks; conducted disaster preparedness exercises for FEMA (CHER-CAP); and developed and conducted exercises for the 8th Civil Support Team at Buckley, AFB, CO, He developed disaster preparedness exercises and classes for the largest US commercial prison system and an international oil and gas corporation.

Command Sergeant Major (CSM) Nickel, retired from the US Army after 27 years of active duty in Special Operations. He participated in numerous deployments and operations, including DESERT ONE in Iran, URGENT FURY in Grenada, DESERT SHIELD/DESERT STORM in Southwest Asia, Operation RESTORE HOPE in Somali 1993, and three deployments to Bosnia. He supported various worldwide joint contingency operations. This included over 15 years of interagency experience with: Department of Energy; NEST-Nuclear Emergency Survey Team; FBI Hostage Rescue Team (HRT); USSS Presidential Protective Division; CIA; and Department of State's Mobile Security Division. He worked and trained with numerous foreign Special Operations units and nine major US metropolitan police departments.

He served on the Joint Staff, J-3 Special Operations Division, Special Activities Branch, coordinating sensitive DOD support with other US agencies.

He was an operator and 'plank holder' assigned to the Army's National Mission Force. He served there for 18 years with assignments on assault and sniper teams, He developed, executed and directed a myriad of emerging tasks and unique missions and assisted in developing Joint SOF doctrine.

Awards and decorations include induction in the USSOCOM Commando Hall of Honor, the Legion of Merit, Outstanding Civilian Career Service Award Medal, two Defense Meritorious Service Medals, Joint Meritorious Civilian Service Award Medal, Meritorious Service Medal, two Joint Service Commendation Medals, Joint Service Achievement Medal, Civilian Service Achievement Medal, plus others, Combat Infantryman Badge, Master Parachutist Badge, Master HALO Wings, Special Forces Tab, SCUBA badge, the Expert Field Medical Badge and foreign jump wings (Korean, Russian, Malaysian).



Resource Reference List

Colorado Federal Executive Board

https://colorado.feb.gov/programs/emergency-management/

National Aeronautics and Space Administration (NASA) Climate Change

NASA's Global Climate Change website hosts an extensive collection of global warming resources for media, educators, weathercasters, and public speakers. For additional information, visit Home – Climate Change: Vital Signs of the Planet (nasa.gov)

Cybersecurity and Infrastructure Security Agency (CISA)

CISA works with partners to defend against today's threats and collaborates to build a more secure and resilient infrastructure for the future. For additional information, visit Homepage | CISA

Federal Emergency Management Agency (FEMA)

Continuity Resource Toolkit

Provides emergency managers with recommendations and best practices on how to analyze local supply chains and work with the private sector to enhance supply chain resilience using a five-phased approach. For additional information, visit Continuity Resource Toolkit | FEMA.gov

Business Continuity Planning suite

https://www.ready.gov/business-continuity-planning-suite

.