Please Note..

This webinar and the engagement tools will be recorded.

An archive will be available on the event website.

NIST | NICE

NICE Webinar: Securing Space- The Next Frontier for Cybersecurity Education and Workforce Development

July 19, 2023

Rodney Petersen

Quincy K. Brown, Ph.D.

Jim McCarthy

Steve Luczynski

NIST | NICE

Securing the Next Frontier for Cybersecurity Education and Workforce Development

Quincy K. Brown, Ph.D.
Director of Space STEM and Workforce Policy
National Space Council

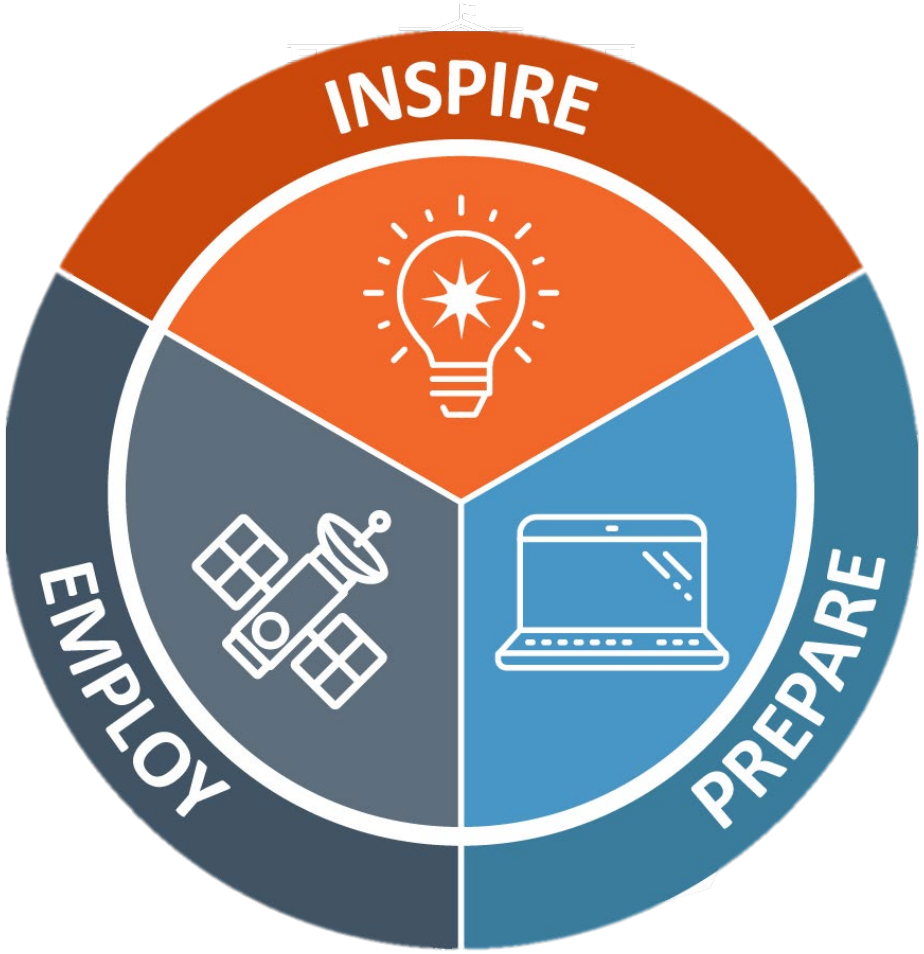
The National Space Council

The National Space Council within the
Executive Office of the President
is charged with providing objective advice to the President
on the formulation and implementation
of space policy and strategy.

National Space Council Membership

- **Chair, Vice President Kamala Harris**
- Secretary of State
- Secretary of Defense
- Secretary of the Interior
- Secretary of Agriculture
- Secretary of Commerce
- Secretary of Labor
- Secretary of Transportation
- Secretary of Energy
- Secretary of Education
- Secretary of Homeland Security
- Director of the Office of Management and Budget
- Director of National Intelligence
- Director of the Office of Science and Technology Policy
- Assistant to the President for National Security Affairs
- Assistant to the President for Economic Policy
- Assistant to the President for Domestic Policy
- Assistant to the President and National Climate Advisor
- Chairman of the Joint Chiefs of Staff
- Administrator of the National Aeronautics and Space Administration (NASA)

Space STEM Focus Areas



Private Sector Commitments and Announcements

Administration Priorities The Record

SEPTEMBER 09, 2022

FACT SHEET: Vice President Harris Announces Commitments to Inspire, Prepare, and Employ the Space Workforce

BRIEFING ROOM › STATEMENTS AND RELEASES

Today, at the second convening of the National Space Council, Vice President Kamala Harris is announcing new commitments from the U.S. government, private sector companies, education and training providers, and philanthropic organizations to support space-related STEM initiatives to inspire, prepare, and employ the next generation of the space workforce.

[Vice President Harris Announces Commitments to Inspire, Prepare, and Employ the Space Workforce]

Inspire

- K-12 media and resources that includes fun, interactive activities for learners
- Resources for educators who teach space-related STEM subjects

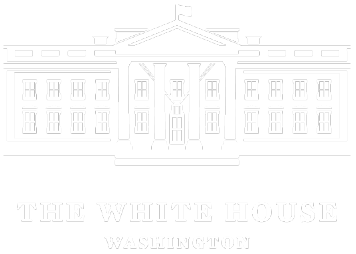
Prepare

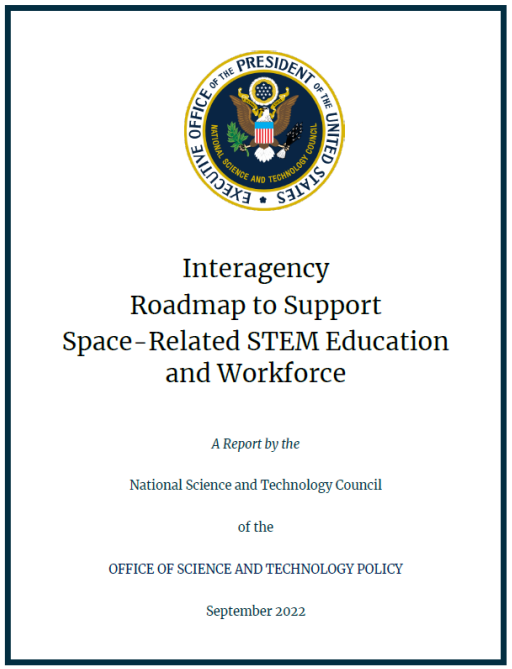
- Skilled technical workforce coalition
- Hands-on learning opportunities

Employ

- Pathways to the space workforce
- Programming for career advancement

Federal Roadmap & Resources





Interagency
Roadmap to Support
Space-Related STEM Education
and Workforce

A Report by the

National Science and Technology Council

of the

OFFICE OF SCIENCE AND TECHNOLOGY POLICY

September 2022

K-12 Space STEM Resources: K-12 Space STEM Resources | Smithsonian Science Education Center

Space Career Guide: Space STEM Career Resources for K-12 Teachers & Students | Smithsonian Science Education Center

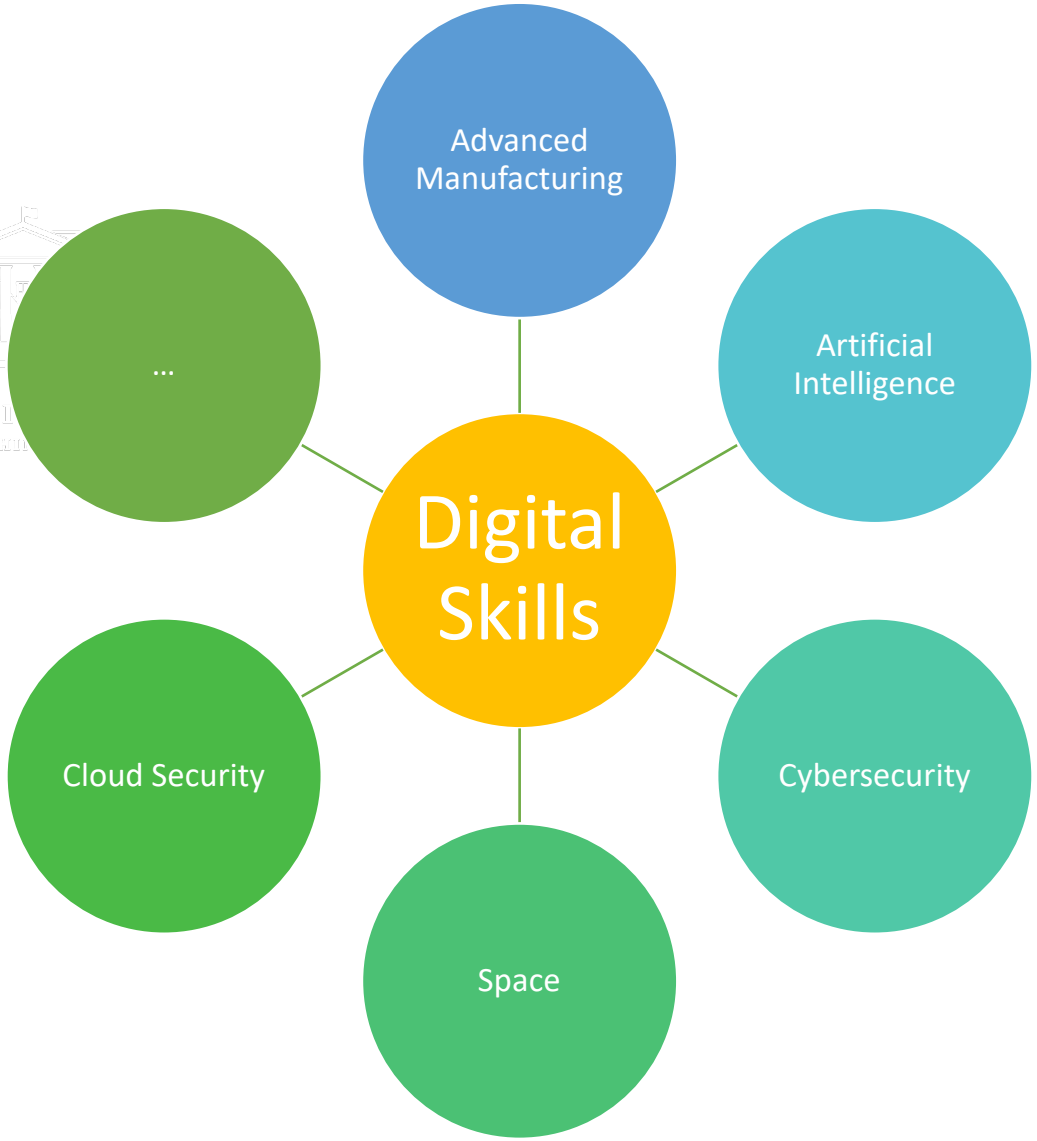
Interagency Roadmap:

Released September 9, 2022

Space Workforce Development

- Career and Career Path Awareness
- Skilled Technical Workforce Coalition
  - Space Coast, Florida
  - New Orleans, Louisiana
  - South Bay, California
- Paid Work-based Learning Opportunities

Common Workforce Development Needs



THANK YOU

THE WHITE HOUSE
WASHINGTON

WH.GOV

Q&A

National Institute of Standards and Technology
U.S. Department of Commerce

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NICE

Applying the Cybersecurity Framework to the Space Eco System

Jim McCarthy NIST
07/19/2023

Who We Are – NIST NCCOE

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

A **solution-driven**, **collaborative** hub addressing complex cybersecurity problems

Who We Are

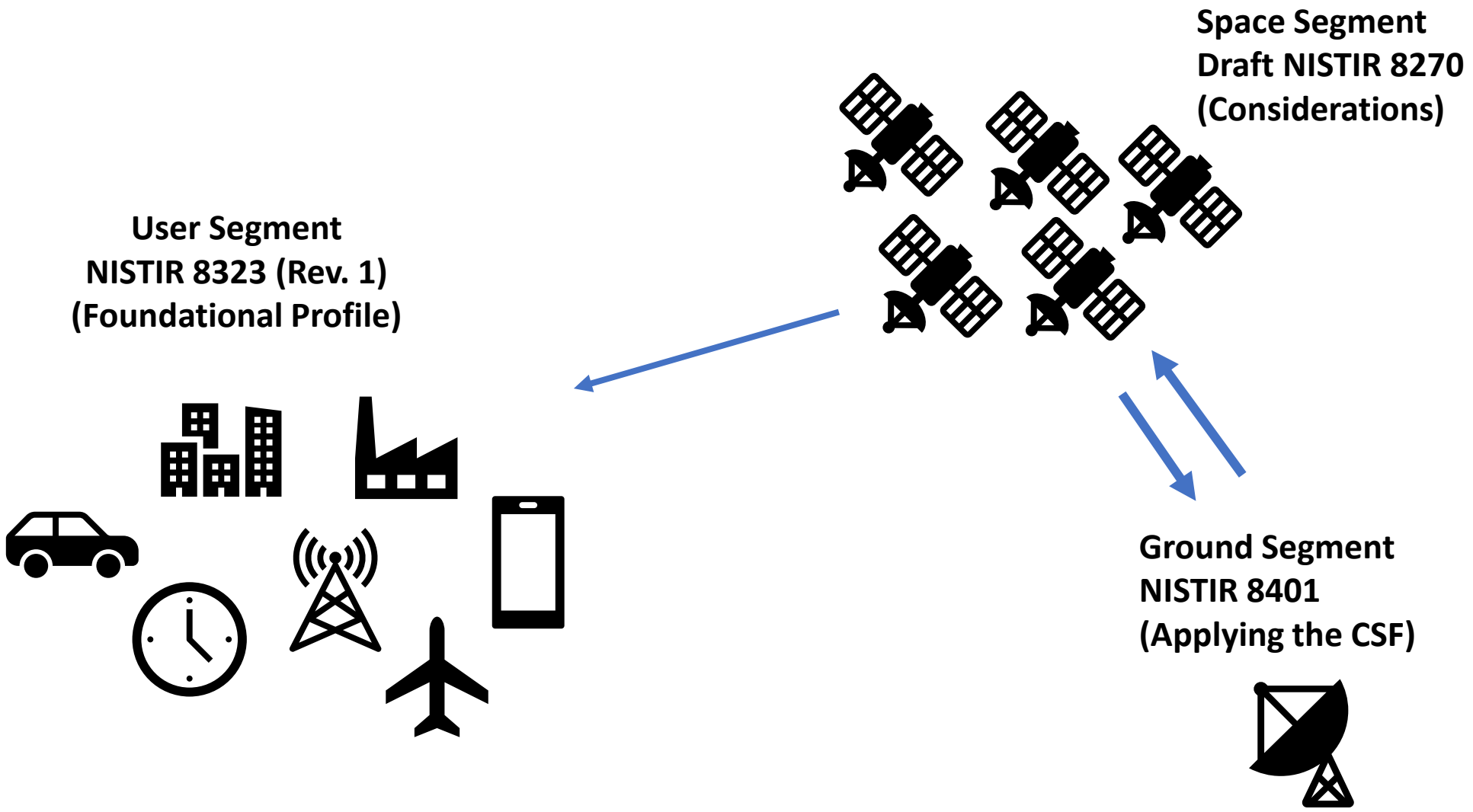
As part NIST, the NCCoE has access to a foundation of **expertise, resources, relationships,** and **experience**

Executive Order 13905: February 12, 2020

Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing (PNT) Services.

- Responsible use of PNT services – deliberate, risk informed use of PNT services
- If disruption or manipulation occurs, minimal impact to national security, economy, public health, and critical functions of Federal Government
- Critical infrastructure – systems/assets so vital to the US that incapacity or destruction could result in debilitating impact
- Directed NIST to Produce PNT Profiles Based on NIST Cybersecurity Framework (CSF)

Cybersecurity Framework (CSF) Profiles



Common Concerns

jamming
An attack that attempts to interfere with the reception of broadcast communications. [CNSSI-4009]

A deliberate communications disruption meant to degrade the operational performance of the RF subsystem. Jamming is achieved by interjecting electromagnetic waves on the same frequency that the reader to tag uses for communication. [NIST-SP-800-98]

The deliberate radiation, reradiation, or reflection of electromagnetic energy for the purpose of preventing or reducing the effective use of a signal. [USG-FRP (Appendix E)]

spoofing
Faking the sending address of a transmission to gain illegal entry into a secure system. [CNSSI-4009]

The deliberate inducement of a user or resource to take incorrect action. Note: Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing. [CNSSI-4009]

Two classes of spoofing include (1) *measurement spoofing*: introduces signal or signal delay that cause the target receiver to produce incorrect measurements of time of arrival or frequency of arrival or their rates of change; and (2) *data spoofing*: introduces incorrect digital data to the target receiver for its use in processing of signals and the calculation of PNT. [DHS-GPS-CI, adapted]

Within the context of this document, spoofing includes manipulation of legitimate GNSS signals with intent to corrupt PNT data or signal measurement integrity. For example, it includes, but is not limited to: the transmission of delayed or false GNSS signals with intent to manipulate an asset's computed position or time and frequency.

The CSF as the Baseline

- The Framework is voluntary,
- Based on existing standards, guidelines, and practices
- Used to manage and reduce cybersecurity risk.
- Helps organizations manage and reduce risks
- Fosters risk and cybersecurity management communications
  Created for the CI community as part of EO 14028.

Content of the PNT Profile

Function

Category

Subcategory

Subcategory ID

CSF language

Guidance on how to apply the subcategory to organizations that rely on PNT services

PNT specific references on how to implement controls to achieve the desired outcomes of the EO

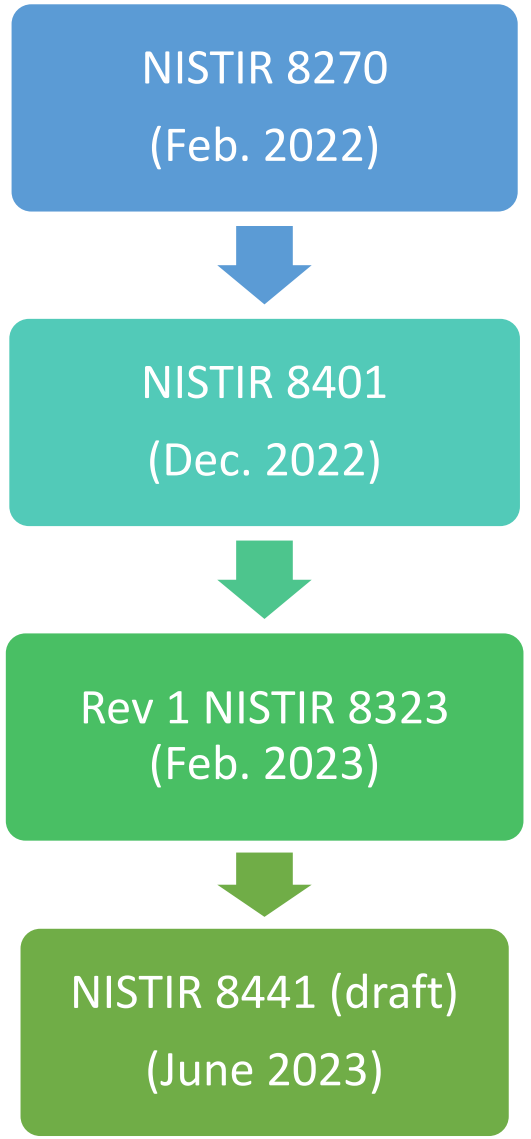
Identify

Asset Management

Subcategory	Applicability to PNT	References (PNT-Specific)
AM-1: **Physical devices and systems within the organization are inventoried.**	Document and maintain an inventory of the PNT system components that reflect the current system. The physical inventory should include PNT system components used to support critical infrastructure/operations and critical system components that rely on PNT data and services to properly function. PNT system components may include GNSS receivers, wireless local area network (WLAN) receivers, terrestrial beacon system receivers (TBS), radio navigation or timing antennas, network switches, Internet of Things (IoT)/ Supervisory Control and Data Acquisition (SCADA) devices, NTP and Precision Time Protocol (PTP) servers, positioning sensors, clocks, etc. Cryptographic modules, test and measurement equipment, navigation systems, etc. are examples of hardware and devices dependent on PNT services. Incorporate a configuration management tool that documents locations of all PNT antennas and verify with physical inspections. During physical inspections, identify equipment associated with PNT devices and locate PNT service provider interfaces, such as GNSS antennas.	**3GPP TS 36.305** 4.3 **DHS CISA** 1.a, 2.a **ICAO 9849** 1.4 **IEEE 1588** 6, 9, 10 **IEEE 802.1AS** 7, 11 **IEEE 2030.101** 4.6, 4.7, 4.8, 4.9 **NIST SP 800-53 Rev. 5** CM-8, CM-9 PM-5 **NIST SP 800-160 Rev. 1** 2.3 **RTCA 229** 2.1.5.2.1, 2.4, 2.5 **RTCA 292** 2.5 **RTCA 326** 3.1 **USG FRP** 1.7.8, 4.4.2, 4.6, 5.1.2, 6

Outcomes and Moving Forward

- Commercial Satellite Operations
  - NSTIR ISTIR 8270: Draft Released 02/2022
- Ground Segment Profile
  - NISTIR 8401: Released 12/2022
  - Focus on Command and Control
- Foundational PNT Profile
  - NISTIR 8323 Original PNT Profile Published: 02/2021
  - NISTIR 8323. Rev 1: Published 02/2023
  - Added Sub-categories and Annexes
- Hybrid Satellite Networks (HSN) Profile
  - NISTIR 8441: Draft Released Public Draft 06/2023
  - Sponsored by Space Systems Command (SSC)
  - Final Profile: 09/2023



NIST NCCOE Cybersecurity Space Domain

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

SECURITY GUIDANCE | OUR APPROACH | NEWS & INSIGHTS | GET INVOLVED | SEARCH

Cybersecurity for the Space Domain

National space assets and operations are critical to the security and economic well-being of the United States. Commercial Space is an increasingly important part of space operations and provide support to other sectors within our critical infrastructure. Space is an inherently harsh environment for operations and space systems are subjected to cybersecurity threats and vulnerabilities. As space becomes a more important to our critical infrastructure, the impact of a cyber attack and the corresponding risk increases. The risk to commercial space operations needs to be understood and managed alongside other risks to ensure safe and successful operations. The NIST Cybersecurity Framework (CSF) has informed the work within this domain at the NCCoE and beyond through interagency agreements (IAA) with our federal partners.

National Institute of Standards and Technology
U.S. Department of Commerce

Join The NIST NCCOE Space Cybersecurity Community of Interest (COI)

spacecyber_nccoe@nist.gov

https://www.nccoe.nist.gov/cybersecurity-space-domain

Q&A

AEROSPACE VILLAGE

Hackers in Cybersecurity Education and Workforce Development

Steve Luczynski
Board Chairman

July 19, 2023

Government and industry attitudes toward security researchers have changed; their willingness to engage is increasing.

Simple, grassroots efforts continue to demonstrate their value.

Building relationships, inspiring others to learn, and promoting the importance of this work is an ongoing process that can help us overcome future challenges and risks.

AEROSPACE VILLAGE .ORG

AEROSPACE VILLAGE

Steve Luczynski
Board Chairman

stevelu@aerospacevillage.org

https://twitter.com/cyberpilot22

https://www.linkedin.com/steveluczynski

https://twitter.com/SecureAerospace

https://www.linkedin.com/company/aerospace-village

aerospacevillage.org

Q&A

Submit an event survey!

https://www.surveymonkey.com/r/July2023NICEWebinar

NIST | NICE

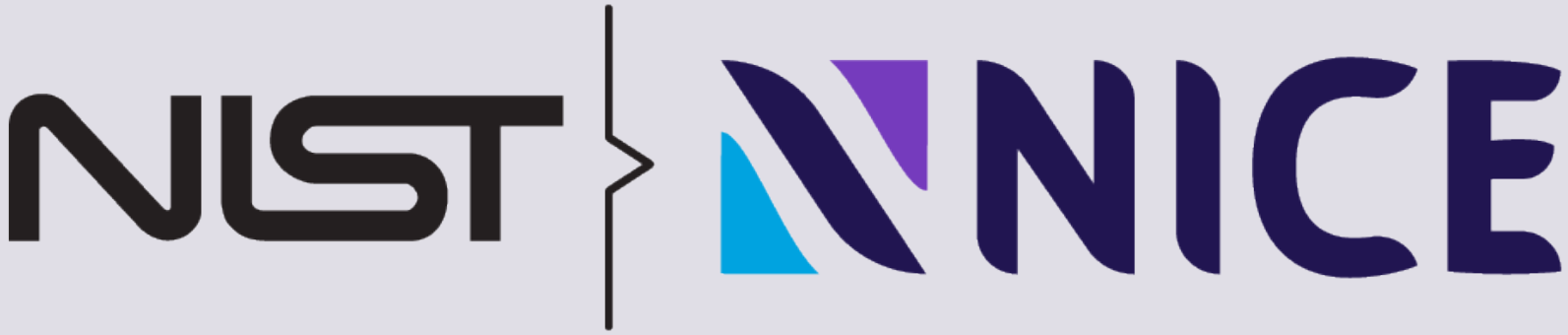
NICE Webinar Series

The Impact of Generative Artificial Intelligence on Education and Workforce

September 20 , 2023, 2-3PM ET

NIST | NICE

nist.gov/nice/webinars


NIST
NICE