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

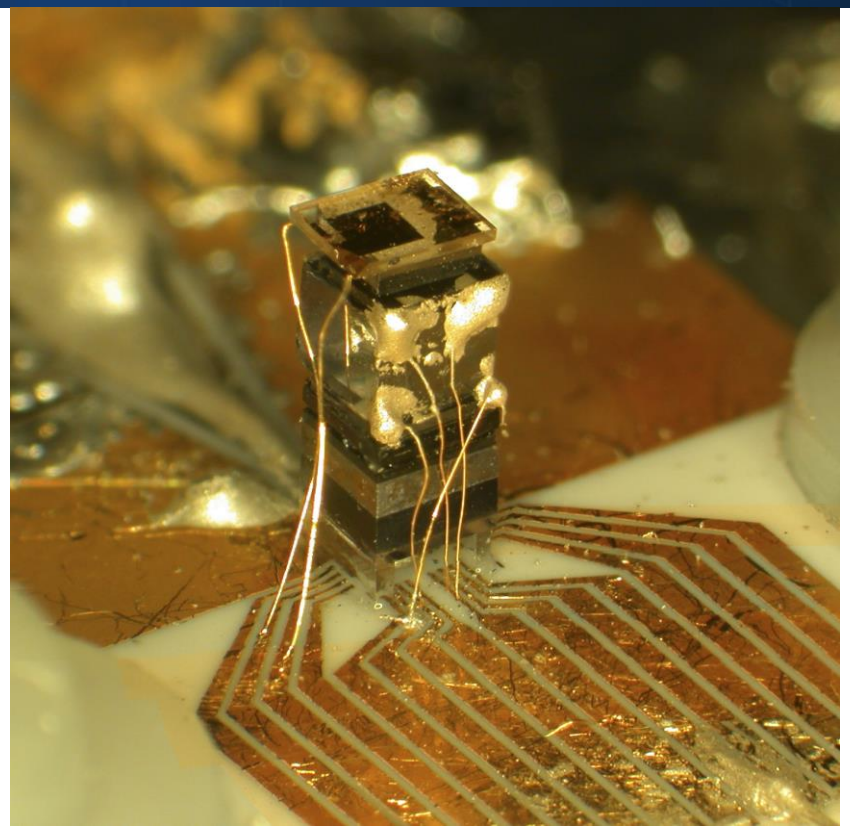
NIST Workshop:
Cybersecurity Framework profile for Ground Segment

June 24, 2021

Agenda

Welcome / Opening Remarks	Suzanne Lightman, NIST
Keynote	Charlie Brown, SMC
NIST and CSF Profile Primer	Suzanne Lightman, NIST
Panel Discussion	Major Rosalva Franco (USSF) Andrew D'Uva (Providence Access Company) Joe DeHaven (DeHaven Consulting Group) JT Thompson (MITRE) Facilitator: Joe Brule (MITRE)
Closing Remarks	Suzanne Lightman, NIST

NIST



An agency of the U.S. Department of Commerce

Working with industry and science to advance innovation and improve the quality of life

NCCoE

The National Cybersecurity Center of Excellence

An FFRDC at NIST

Accelerating the deployment and use of secure, standards-based technologies

Purpose

Executive Order 13905 of February 12, 2020

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

"Because of the widespread adoption of PNT services, the disruption or manipulation of these services has the potential to adversely affect the national and economic security of the United States. To strengthen national resilience, the Federal Government must foster the responsible use of PNT services by critical infrastructure owners and operators."

Industry Participation

Engage With Us

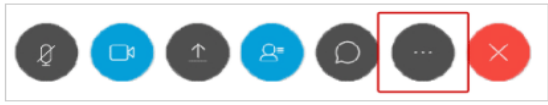
We want to hear from industry!
Please share your questions, thoughts and comments via the Q&A panel on the Webex Platform

Q&A

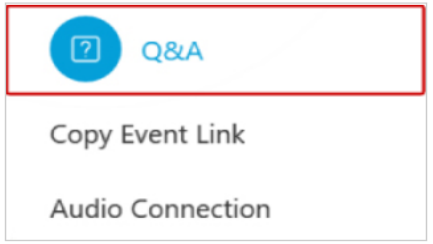
How to find

1 In the toolbar at the bottom, click on the 3-dot button

2



On the menu, click Q&A



3 Type your question in the box

4 Click **send** or **send privately**

Keynote:
Charlie Brown

Overview of NIST Cybersecurity Framework

NIST Cybersecurity Framework

- Common and accessible language
- Adaptable to many technologies, lifecycle phases, sectors, and uses
- Risk-based
- Meant to be paired
- Living document
- Guided by many perspectives – private sector, academia, public sector

NIST Cybersecurity Framework

Three Primary Components

Core

Desired cybersecurity outcomes organized in a hierarchy and aligned to more detailed guidance and controls

Implementation Tiers

A qualitative measure of organizational cybersecurity risk management practices

Profiles

Alignment of an organization's requirements and objectives, risk appetite and resources ***using*** the desired outcomes of the Framework Core

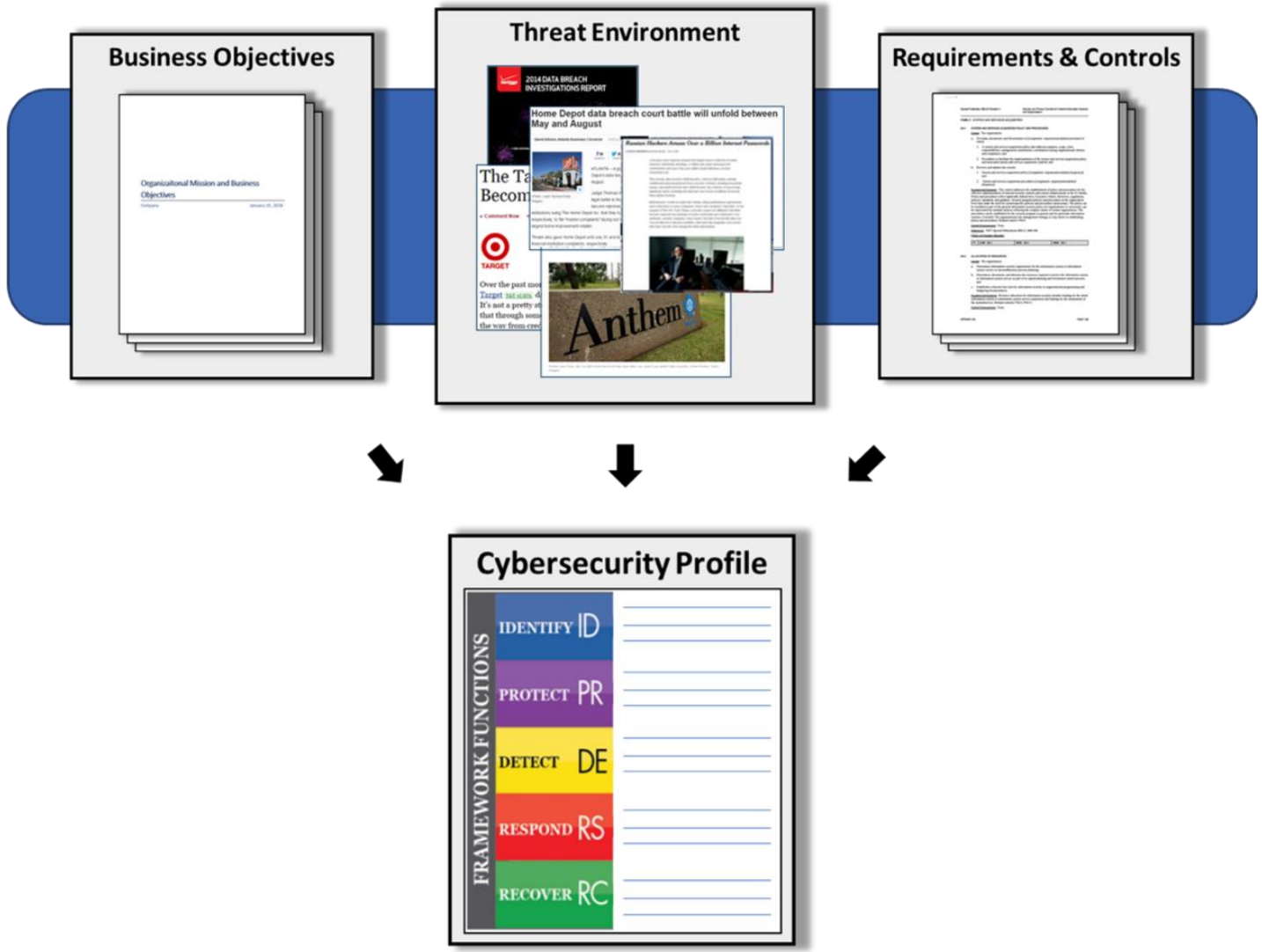
Framework Core

Establishes a Common Language

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Cybersecurity Framework Profiles



Cybersecurity Framework Profile - Examples

Manufacturing Profile

NIST Discrete Manufacturing Cybersecurity Framework Profile

Cybersecurity Framework Smart Grid Profile

Cybersecurity Framework Smart Grid Profile

PNT End User Profile

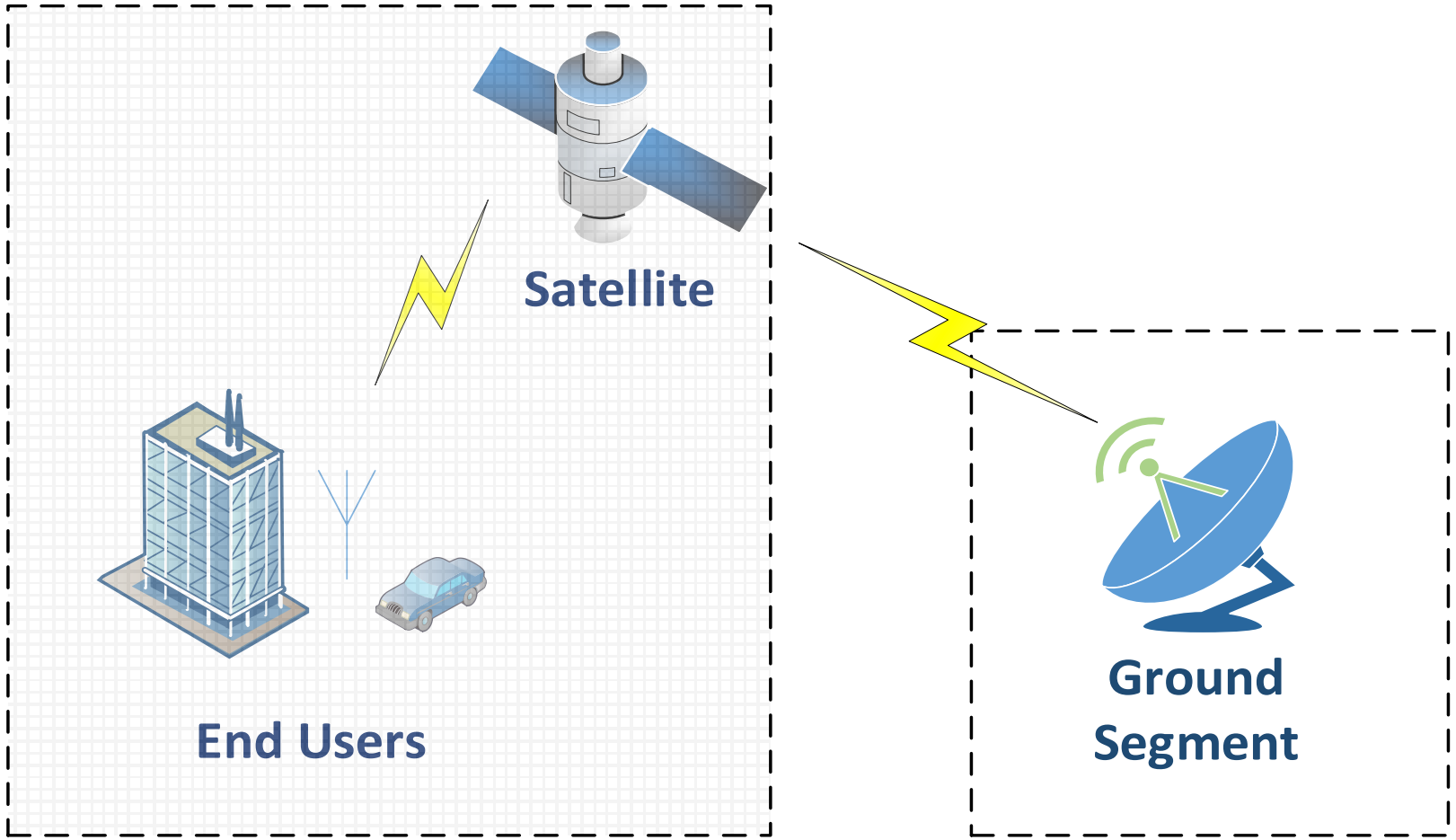
Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services

Additional Resources: https://www.nist.gov/cyberframework/resources/risk-management-resources

Profile Objectives

- Provide a foundational profile to support a wide range of stakeholders in increasing the cybersecurity of the ground segment
- Profile focus is on cybersecurity
- Flexible enough to facilitate tailoring to specific enterprises' environments
- Engage with primary stakeholders, both public and private, to inform development of the profile
- Focus on commercial operators

NIST Profile Scope



Profile: Target Audience

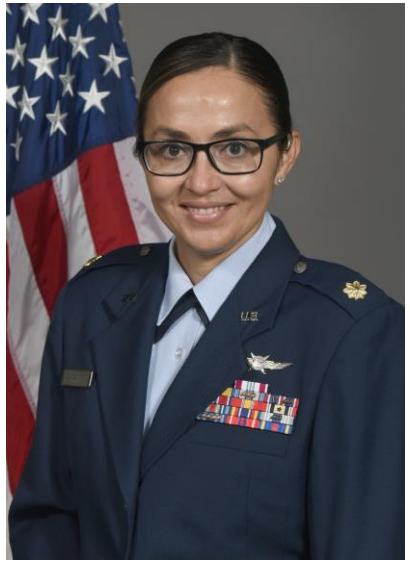
- Commercial satellite operators
- Satellite risk managers/cybersecurity professionals
- Mission and business owners
- Researchers

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

NIST Ground Segment Workshop

Facilitated Panel Discussion

Today's Panel



Major Rosalva Franco
USSF
Chief, Defense Cyber Operations, Space Production Corps, Space and Missile Systems Center

Andrew D'Uva
Providence Access Company
25+ years international commercial satellite and telecommunications

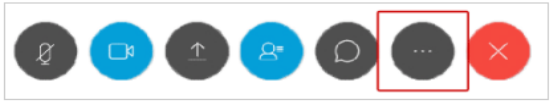
Joe DeHaven
DeHaven Consulting Group
40+ years industry experience including Director Space INFOSEC

JT Thompson
MITRE
20 years supporting cybersecurity capabilities with the USSF, and operational effectiveness of space functionality

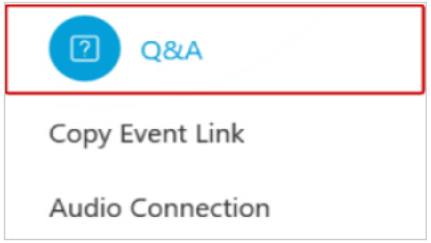
Q&A

How to find

1 In the toolbar at the bottom, click on the 3-dot button



2 On the menu, click Q&A



3 Type your question in the box

4 Click **send** or **send privately**

Engage with us

Please share your questions via the Q&A panel on the Webex Platform

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

Thank You Very Much!

We want to hear from you!

Please tell us your thoughts, comments and follow-up questions on this workshop and your cybersecurity efforts.

Please reach out to us at:

gps-NCCOE@nist.gov