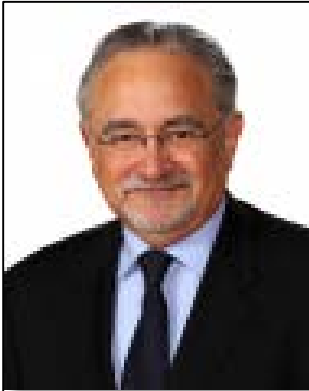


The FCC Communications Security, Reliability and Interoperability Council (CSRIC) WG4: What We Can Learn



Moderator

Ron Clifton, CISSP

Senior Solutions Architect
Media & Entertainment
Tata Communications



Donna Bethea-Murphy

SVP Global Regulatory,
Inmarsat Global, Ltd



**Seton Droppers,
CISSP**

Independent Consultant
& CSO/Director
Enterprise Security



Philip Schoene

VP Operations
Public Broadcasting
Service (PBS)



Ron Tencati

Delivery Consultant,
Rolta Advisex

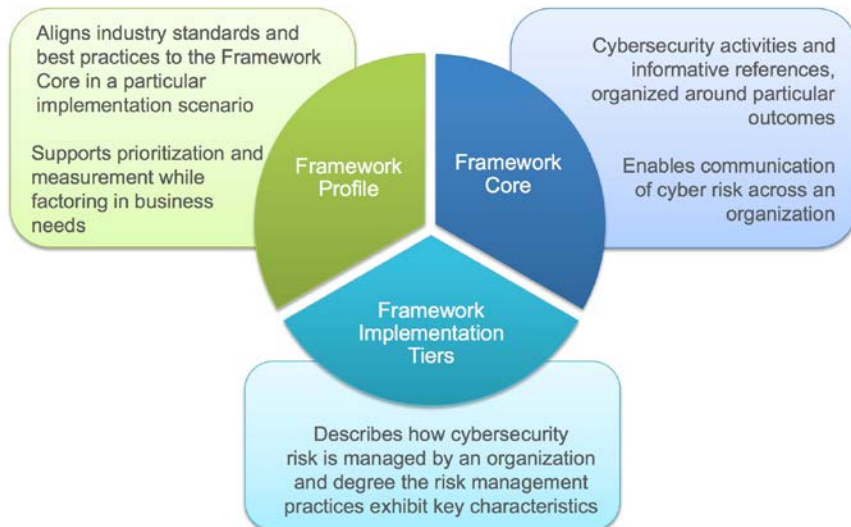
The NIST Cybersecurity Framework

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

Cybersecurity Framework Components



FRAMEWORK FUNCTIONS	IDENTIFY ID	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
	PROTECT PR	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
	DETECT DE	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
	RESPOND RS	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
	RECOVER RC	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES

Figure 1: Framework Core Structure

The NIST Cybersecurity Framework

Table 2: Function and Category Unique Identifiers

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

CSC= CIS
Critical Security Controls

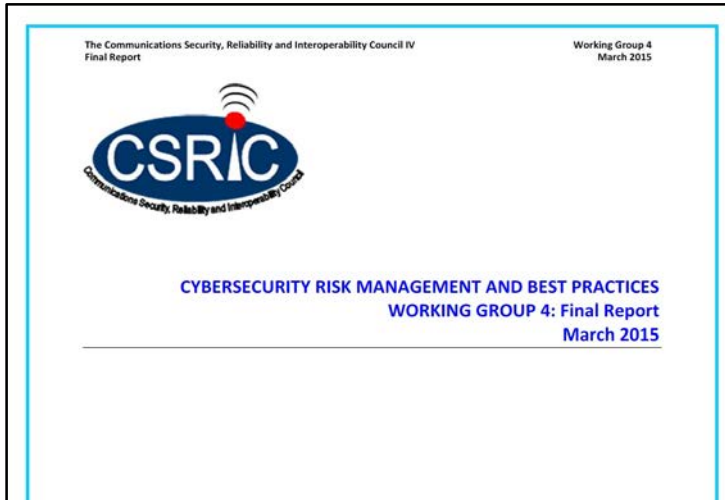
Function	Category	Subcategory	Informative References
		restoration of systems or assets affected by cybersecurity events.	<ul style="list-style-type: none"> NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8
		Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned	<ul style="list-style-type: none"> COBIT 5 BAI05.07 ISA 62443-2-1:2009 4.4.3.4 NIST SP 800-53 Rev. 4 CP-7, IR-4, IR-8
		Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events	<ul style="list-style-type: none"> COBIT 5 BAI01.10 CCS CSC 18 ISA 62443-2-1:2009 4.3.4.5.1 ISO/IEC 27001:2013 A.16.1.5 NIST SP 800-53 Rev. 4 CP-7, CP-10, IR-4, IR-8
		monitored to detect potential cybersecurity events	<ul style="list-style-type: none"> NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20 ISA 62443-3-3:2013 SR 6.2 ISO/IEC 27001:2013 A.12.4.1
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	<ul style="list-style-type: none"> NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20

Table 3: Framework Core

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	<ul style="list-style-type: none"> CCS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	<ul style="list-style-type: none"> CCS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: Organizational communication and data flows are mapped	<ul style="list-style-type: none"> CCS CSC 1 COBIT 5 DSS06.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	<ul style="list-style-type: none"> CCS CSC 1 COBIT 5 APO03.03 ISO/IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value	<ul style="list-style-type: none"> COBIT 5 APO03.03, APO03.04, BAI09.02 ISA 62443-2-1:2009 4.2.3.6 ISO/IEC 27001:2013 A.8.2.1 NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	<ul style="list-style-type: none"> COBIT 5 APO01.02, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1

ISO 27001

CSRIC WG 4 – Cybersecurity Risk Management & Best Practices




Cybersecurity Risk Management and Best Practices (WG 4)

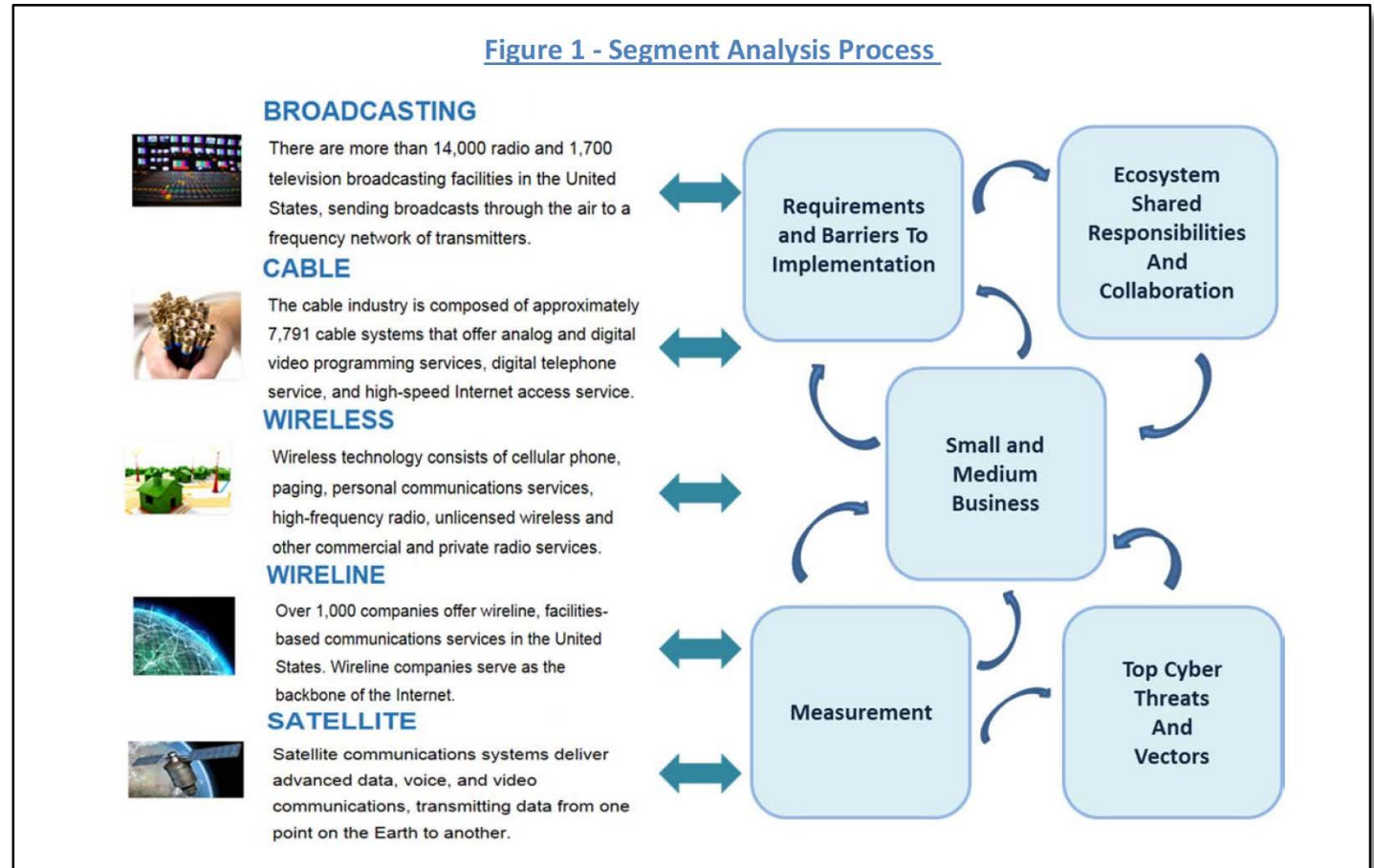
Cybersecurity Framework for the Communications Sector

Final Report Presentation
March 18, 2015

Co-Chairs:
Robert Mayer, USTelecom
Brian Allen, Time Warner Cable







9.1 Broadcast Segment

- Local Broadcast Station
- Local Small Radio Station
- Broadcast Network
- Broadcast Hubbed Operation

The Communications Security, Reliability and Interoperability Council IV
Final Report

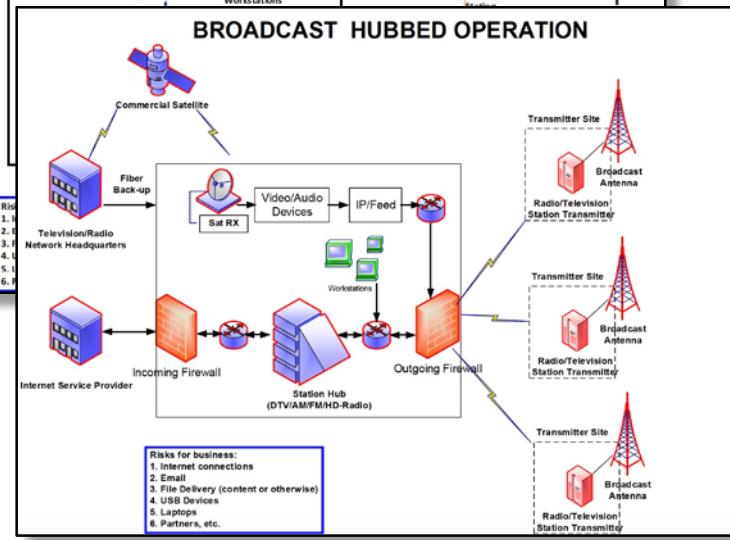
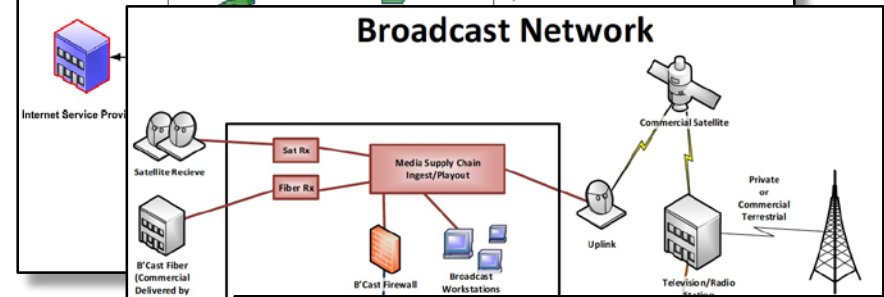
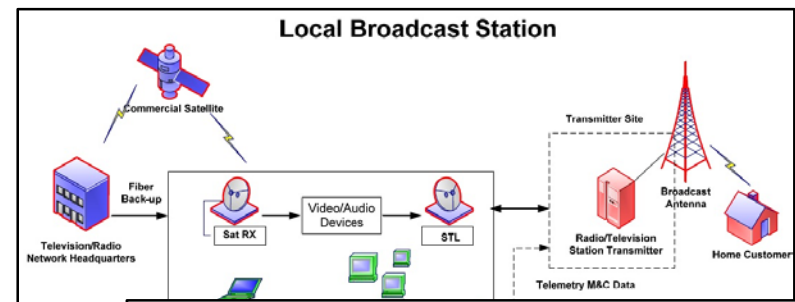
Working Group 4
March 2015



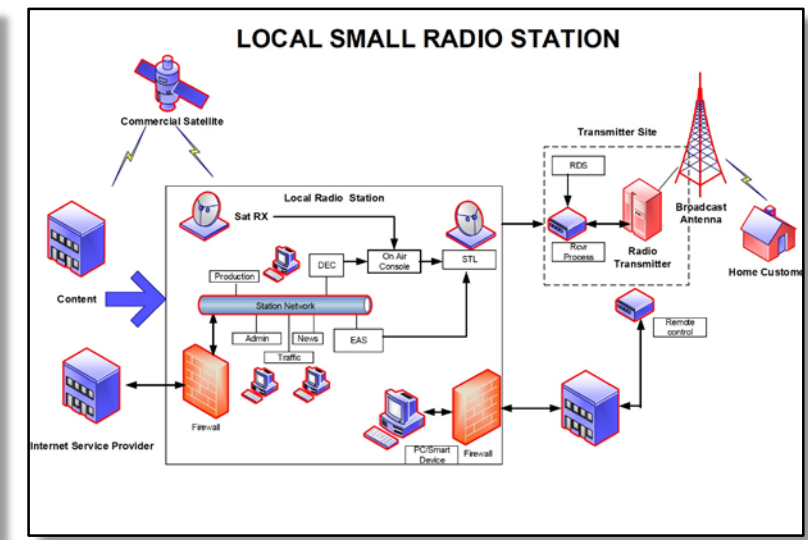
9.1 BROADCAST SEGMENT
CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES
WORKING GROUP 4
March 2015

III. BROADCAST SEGMENT GROUP MEMBERS

Member	Company
Adrienne Abbott	Nevada Association of Broadcasters
Sohail Anwar	National Public Radio
Edward Czarnecki	Monroe Electronics, Inc. / Digital Alert Systems
Seton Droppers	Public Broadcasting System
Christopher Homer	Public Broadcasting Service
Robert Ross	CBS Television Network
David Williams	National Public Radio
Kelly Williams	National Association of Broadcasters



- Risks for business:
1. Internet connections
 2. Email
 3. File Delivery (content or otherwise)
 4. USB Devices
 5. Laptops
 6. Partners, etc.



9.3 Satellite Segment



The Communications Security, Reliability and Interoperability Council IV
Final Report

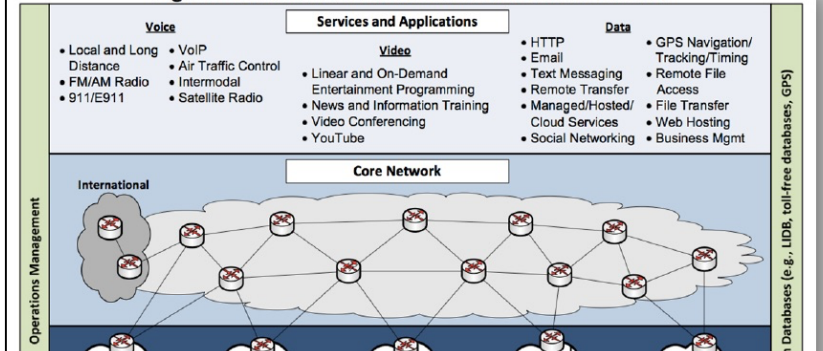
Working Group 4
March 2015

9.3 SATELLITE SEGMENT CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES WORKING GROUP 4 March 2015

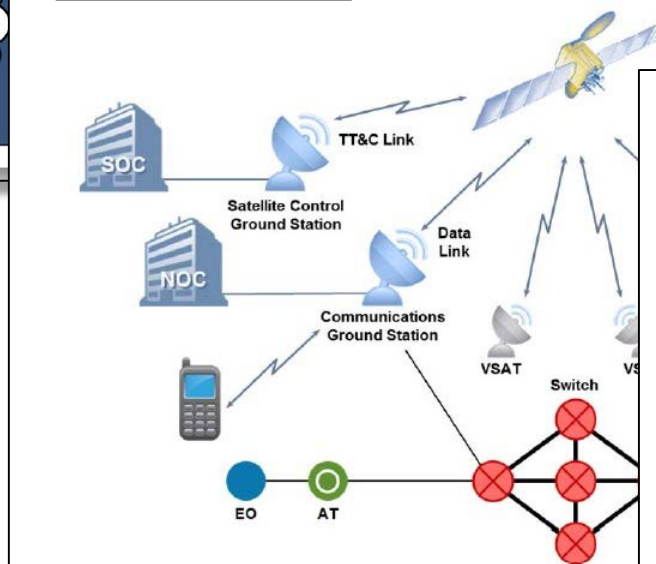
Satellite Segment Subgroup Members

Name	Company
Donna Bethea Murphy - Chair	Iridium Communications Inc.
Anthony Acosta	Northrop Grumman
Andre Christian	O3b Government
Shelton Darensburg	ViaSat
Steve Doiron	Echostar/Hughes Network Systems
Vinit Duggal	Intelsat
Andrew D'Uva	Providence-Access
Victor Einfeldt	Iridium Communications Inc.
Rick Foster	Lockheed Martin
Aniruddha Karmarkar	Lockheed Martin
Greg Kulon	Boeing
Ethan Lucarelli	Wiley Rein LLP
Jennifer Manner	Echostar
Martin Pitson	Telesat
Joel Rademacher	Iridium Communications Inc.
Alan Rinker	Boeing
Derek Schatz	Boeing
J.J. Shaw	O3b Government
Fred Travis	Iridium Communications Inc.

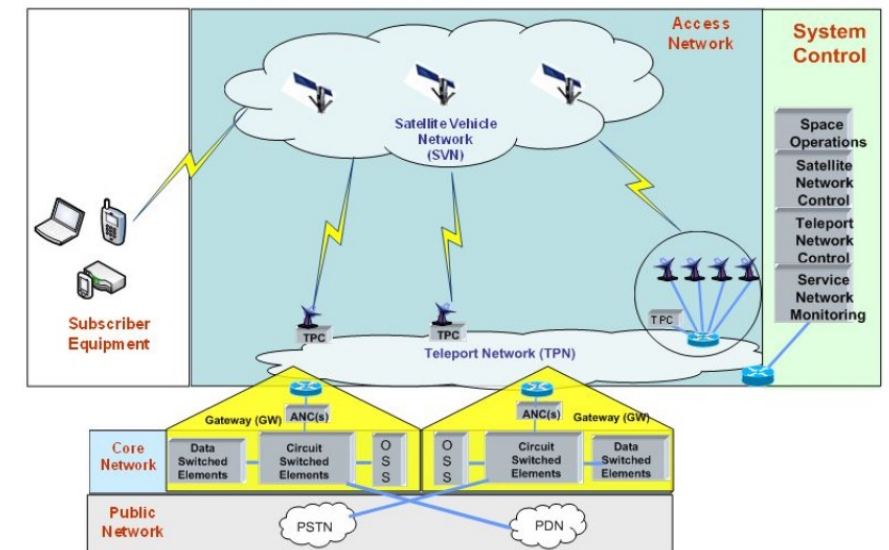
Figure 2-2: Communications Sector Architecture Model



Fixed Satellite Service (FSS)



Mobile Satellite Service (MSS)

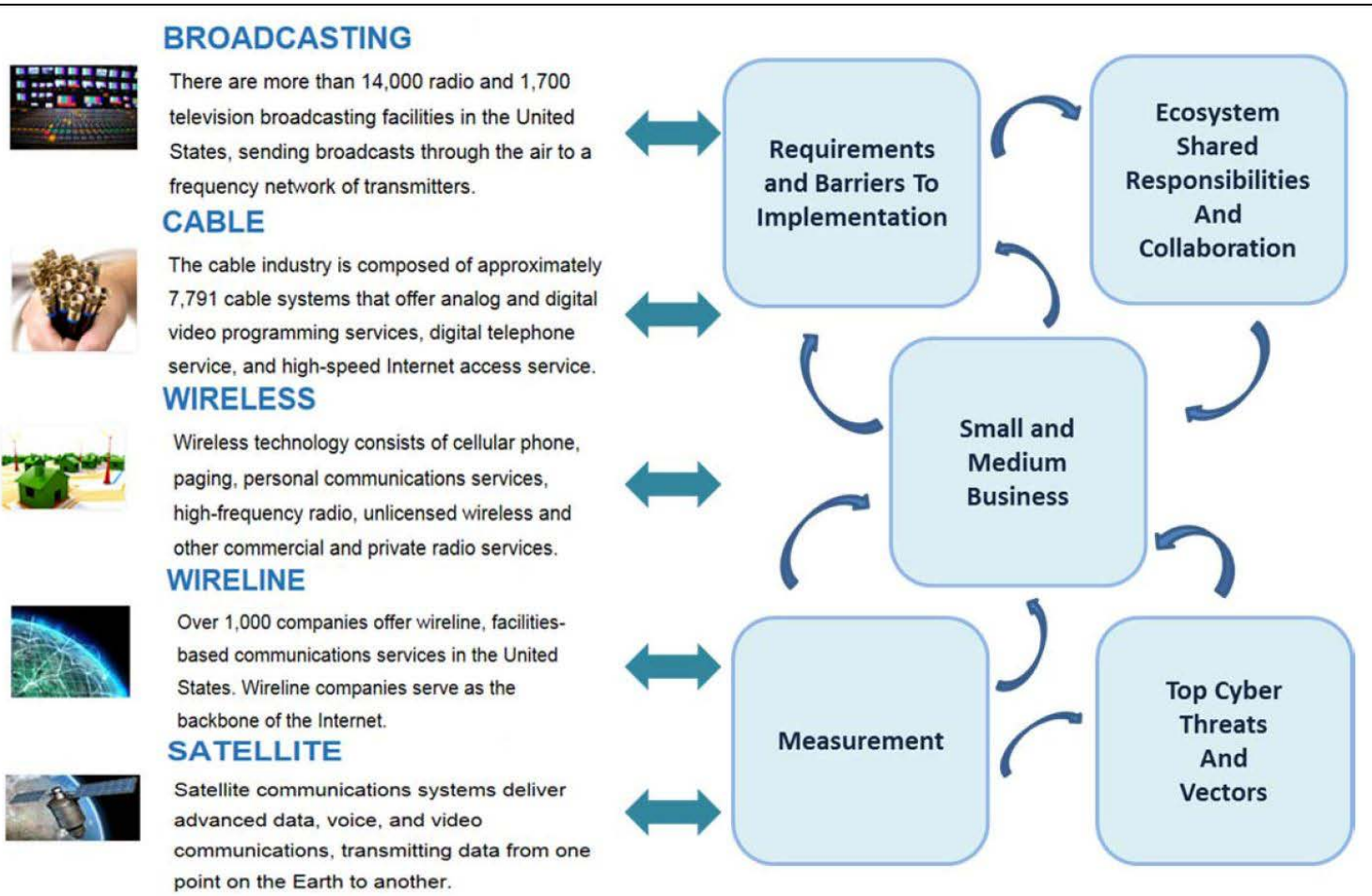


- Communications Sector Architecture Model
- Fixed Satellite Services
- Mobile Satellite Services



Donna Bethea-Murphy

SVP Global Regulatory, Inmarsat Global, Ltd



Seton Droppers, CISSP®

Communicator | Visualizer | Problem Solver | Systems | Networks | Processes

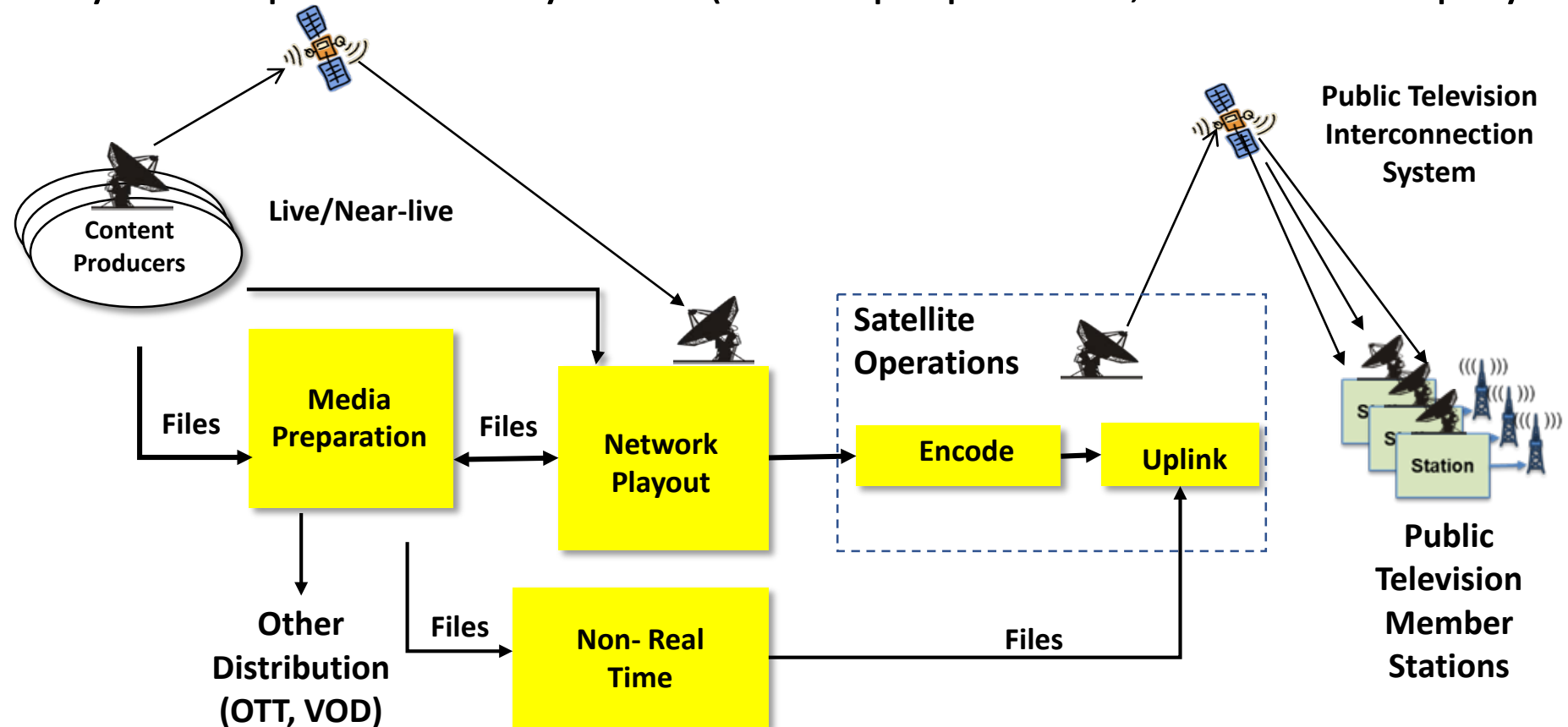


Senior Cyber Security professional passionately working with multiple stakeholders and customers building practical combinations of installed and innovative technologies that ensure security and reduce unplanned interruptions and down-time.

PBS Distribution Operations

Cyber Security priorities:

- Protect the integrity and availability of the content
- Maintain the availability of the production systems (media preparation, transfer and playout)



Federal Communications Commission

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014

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



CSRIC IV
WG4

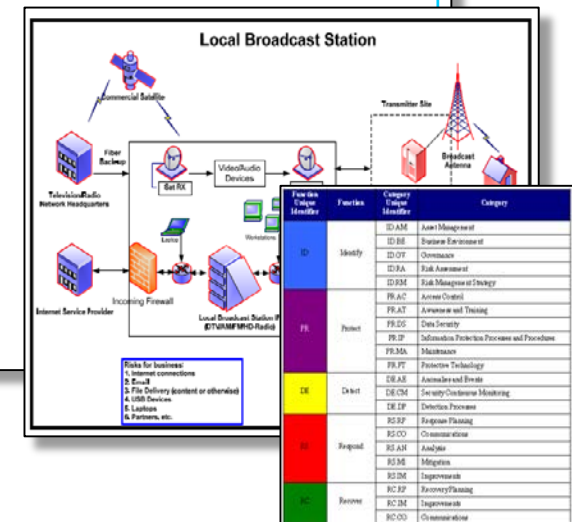


The Communications Security, Reliability and Integrity Council IV
Final Report

Working Group 4
March 2015



CYBERSECURITY RISK MANAGEMENT AND BEST PRACTICES
WORKING GROUP 4: Final Report
March 2015



Industry-Specific Requirements

NIST
SP800-53a

Questions and Answers



Moderator

Ron Clifton, CISSP

Senior Solutions Architect
Media & Entertainment
Tata Communications



Donna Bethea-Murphy

SVP Global Regulatory,
Inmarsat Global, Ltd



**Seton Droppers,
CISSP**

Independent Consultant
& CSO/Director
Enterprise Security



Philip Schoene

VP Operations
Public Broadcasting
Service (PBS)



Ron Tencati

Delivery Consultant,
Rolta Advisex