Partnering to Advance Trusted and Holistic Spectrum Solutions (PATHSS) – Introducing Dynamic Spectrum Sharing (DSS)
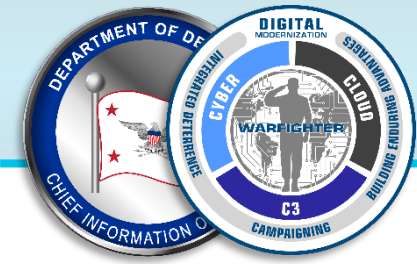
DoD CIO, C3, EMSEPP

8 April 2024
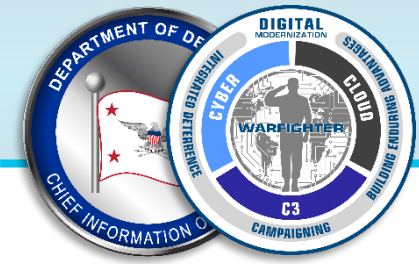
Welcome

Agenda

Welcome

- Ms. Meredith Attwell Baker (CTIA)
- Hon. Sherman (DoD CIO)
- Lt. Gen. Isaacson (JSJ6)

Break – 15 Min

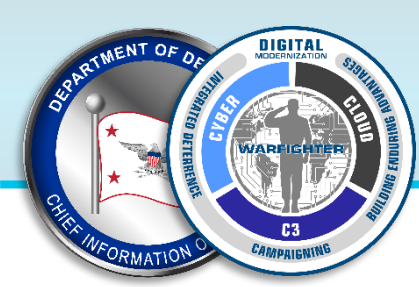Dynamic Spectrum Sharing (DSS) Framework

- Mr. Matthew Pearl (EOP/NSC)
- Mr. Kevin Mulvihill (DoD CIO C3)
- Dynamic Spectrum Sharing (DSS) Framework

National Spectrum Consortium (NSC) & PATHSS Overview

- NSC Overview
- PATHSS

Next Steps

Questions

Mrs. Meredith Attwell Baker
President and CEO, CTIA

Meredith Attwell Baker joined CTIA as its President and CEO in June 2014. She brings Extensive experience on spectrum issues and wireless policy and a keen understanding government and business must work together to drive innovation. Prior to joining CTIA, Mrs. Baker served as the Senior Vice President of Government Affairs at Comcast NBC Universal where she was responsible for developing policy positions on legislative and regulatory issues and representing those positions before the U.S. Congress, the Administration and government agencies. Appointed by President Barack Obama in 2009, Mrs. Baker served as a Commissioner to the Federal Communications Commission (FCC) until June 2011. During her tenure, she championed a forward-looking approach to spectrum management issues as well as a flexible regulatory environment to encourage continued innovation and competition in the technology and telecommunications industries. Prior to joining the FCC, Mrs. Baker served in the Bush Administration as the Acting Assistant Secretary of Commerce for Communications and Information as well as the Acting Administrator of the National Telecommunications and Information Administration (NTIA). While at NTIA, she facilitated the nation's historic transition to digital television, which freed commercial spectrum for wireless companies; promoted market-based policies that encouraged innovation; served on delegations representing the United States at major international telecommunications conferences; and engaged in bilateral discussions with senior level officials from countries around the world to encourage investment in the United States.
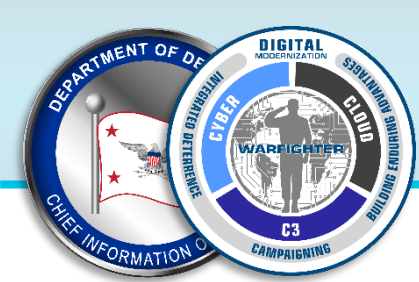
Honorable John Sherman
Department of Defense Chief Information Officer

Mr. John Sherman was sworn in as the Department of Defense Chief Information Officer (DoD CIO) on December 17, 2021. In this role he is the principal advisor to the Secretary of Defense for Information Management / Information Technology (IT) and Information Assurance, as well as non-intelligence space systems; critical satellite communications, navigation, and timing programs; spectrum; and telecommunications matters. Prior to assuming his duties, he served as the Acting DoD CIO and Principal Deputy, DoD CIO from June 2020 to September 2021. Before joining the Department, Mr. Sherman served as the Intelligence Community (IC) CIO from 2017-2020. In this position driving and coordinating IT modernization among 17 agencies, he led major advancements to the IC's cloud computing, cybersecurity, and interoperability capabilities. He built long-term commitment to these priorities among stakeholders, both in government and industry, and ensured that the IC would remain a leader in each of these areas. Prior to his tour as the IC CIO, Mr. Sherman served from 2014-2017 as the Deputy Director of the Central Intelligence Agency's (CIA's) Open Source Enterprise (OSE), where he helped transform Open Source Intelligence, leveraging new technologies and interagency partnerships to enhance the growing OSE mission. He previously served for seven years in several senior executive positions at the National Geospatial-Intelligence Agency (NGA), where he led organizations involved in analysis, collection, homeland security, organizational strategy, and international affairs. Earlier, he served as the Principal Deputy National Intelligence Officer for Military Issues on the National Intelligence Council, and as a White House Situation Room duty officer. Mr. Sherman began his IC career in 1997 as an imagery analyst.
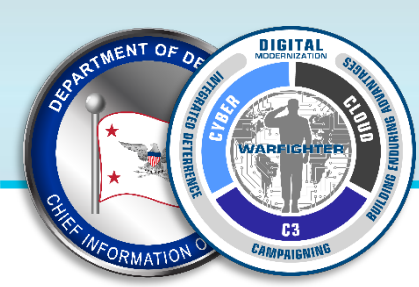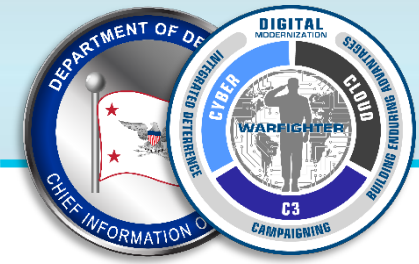
Lt. Gen. David "Todd" Isaacson
Dir. for C4/Cyber, Chief Information Officer, J-6

LTG David T. (Todd) Isaacson assumed his current position as the Director for Command, Control, Communications, and Computers/Cyber, and Chief Information Officer, J-6, Joint Chiefs of Staff on 18 December 2023. In this role, he develops C4 capabilities, conducts analysis and assessments, provides Joint and Combined Force C4 guidance, and evaluates C4 requirements, plans, programs, and strategies for the Chairman of the Joint Chiefs of Staff. He has previously served in the Joint Staff J-6 as a Division Chief focused on interoperability. LTG Isaacson was born in Fort Monroe, Virginia. He graduated from Auburn University in April 1988 with a Bachelor of Science in Electrical Engineering and was commissioned through The Reserve Officer Training Corps as a Signal Officer. After graduation from the Signal Officer Basic Course, he as assigned to the 50th Signal Battalion (Airborne) at Fort Bragg, North Carolina, where he served as a Platoon Leader, Company Executive Officer, Battalion Operations Officer, and Company Commander. Following the Signal Officer Advanced Course, he served with the 160th Special Operations Aviation Regiment (Airborne) as a battalion Signal Officer and Operations Officer. Upon Completing Command and General Staff College and a master's degree in Telecommunications, LTG Isaacson returned to Fort Bragg and served as the Regimental Signal Officer for the 505th Parachute Infantry Regiment and Battalion S-3 (Operations) for the 82nd Signal Battalion (Airborne). He was then assigned to the Combat Applications Group where he served as the Signal Squadron Commander and was subsequently assigned to the Joint Special Operations Command as the J-6 Operations Officer. LTG Isaacson then commanded the 50th Expeditionary Signal Battalion (Airborne). After attending the U.S. Army War College in Carlisle, Pennsylvania, he was assigned to the Department of the Army G-3/5/7 LandWarNet Battle Command Directorate where he served as the Current Operations Division Chief. After LTG Isaacson served as Deputy Commanding General, Army Network Enterprise Technology Command. He then served as Deputy Chief of Staff, G-6, U.S. Army Forces Command, Fort Bragg, North Carolina. Following this assignment, he served as the Director of Networks, Services and Strategy, Headquarters, Department of the Army, Chief Information Officer (CIO)/G-6 from 2018 to 2020. Additionally, LTG Isaacson then served as the United States Cyber Command Chief of Staff from July 2020 to June 2022. Prior to his current assignment as the Director J-6, he served as the Joint Staff J-1 Director.

Break - 15 min
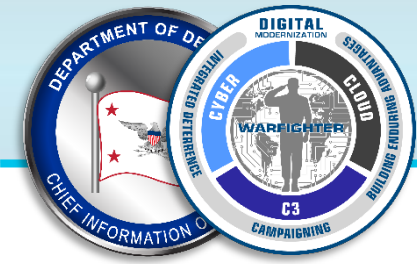
Agenda

Welcome

- Ms. Meredith Attwell Baker
- Hon. Sherman (DoD CIO)
- Lt. Gen. Isaacson (JSJ6)

Break – 15 Min
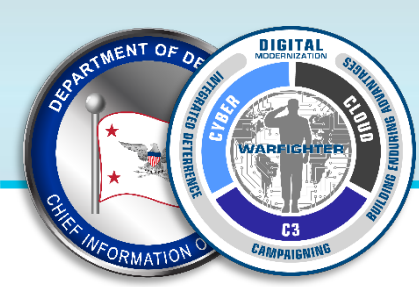
Dynamic Spectrum Sharing (DSS) Framework

- Mr. Matthew Pearl (EOP/NSC)
- Mr. Kevin Mulvihill (DoD CIO C3)
- Dynamic Spectrum Sharing (DSS) Framework

National Spectrum Consortium (NSC) & PATHSS Overview
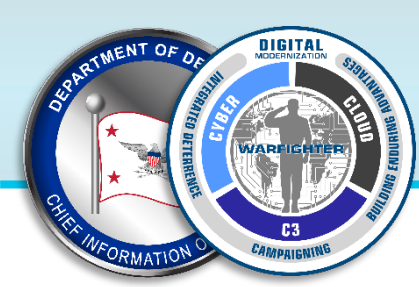
- NSC Overview
- PATHSS

Next Steps

Questions

Dynamic Spectrum Sharing Framework

- Mr. Matthew Pearl
- Mr. Kevin Mulvihill
- Col Steven Trueblood

Matt Pearl serves as Director and Special Advisor for Emerging Technologies at the White House National Security Council, where focuses on technology and telecommunications issues, including spectrum policy, Open RAN, 5G, and IoT; global standards setting; cybersecurity of telecom networks; and data security. Immediately before serving at the NSC, Matt was an Associate Bureau Chief at the Federal Communications Commission (FCC). At the FCC, he was responsible for managing numerous spectrum transitions, including 3450-3550 MHz, 3.5 GHz/CBRS, 3.7-4.2 GHz (C-Band), and several millimeter waves bands. He also managed many of the Bureau's nearly two million spectrum licenses. From 2014 until 2020, Matthew was a Research Affiliate at the Berkman-Klein Center for Internet and Society at Harvard University, where he was part of an effort to advance mesh network technologies, and to evaluate the legal, policy, and technological issues that are raised by the adoption of such networks. In 2010, Matthew earned a J.D. at Yale Law School, where he served as a submission's editor for the Yale Journal on Regulation. Before joining the FCC, he worked as a law clerk for Judge Harris Hartz of the United States Court of Appeals for the Tenth Circuit. Prior to that, he was a law clerk for Judge Lawrence Kahn of the United States District Court for the Northern District of New York.
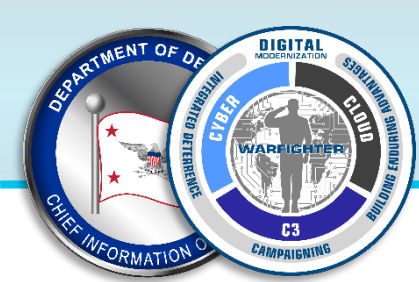
Mr. Kevin Mulvihill
Dep. CIO for Command, Control, & Communications

Kevin Mulvihill is a member of the Senior Executive Service, and the Deputy Chief Information Officer for Command, Control, and Communications (C3), Office of the Secretary of Defense, Chief Information Officer. He provides strategic direction, policy guidance, and oversight to enable the Department to effectively define, prioritize, acquire, govern, manage, and implement C3 capabilities in support of DoD operations. As DCIO, Mr. Mulvihill provides policy and guidance to execute Principle Staff Assistant responsibilities for: spectrum; communications systems and networks; C2 and coalition information sharing capabilities; Position, Navigation and Timing (PNT); Tactical Network Management; Waveform Management; and Enterprise Mobility. He leads teams responsible for the horizontal and vertical integration of operational level C2 and strategic command, control and communications, supporting joint and coalition concepts of operations. Prior to his current assignment, Mr. Mulvihill led modernization efforts for DoD Satellite Communications, data links and tactical communication capabilities in support of warfighter needs for the DoD CIO. Additionally, Mr. Mulvihill served as the Net-Centric Capability Portfolio Manager, Secretary of the Air Force, Office of Chief Information Officer (CIO) Headquarters Air Force, Pentagon, Washington, DC., where he directed integration efforts for all net-centric Air Force Space/C4ISR/Cyber warfighting capabilities. He provided wide-ranging leadership for managing and unifying the entire portfolio of Net-centric capabilities, Air Force-wide. Mr. Mulvihill has held a variety of leadership positions in civilian and military arenas, focusing primarily on operations and requirements planning of DoD C2 systems at the tactical, operational, and strategic level of warfare. He began his government service career upon graduation from Lewis University in Joliet, Illinois, where he earned a Bachelor of Science Degree with Honors in Aviation Maintenance Management. He was commissioned and served in the United States Air Force in a variety of operational and staff positions, commanding an E-3 Sentry squadron and leading coalition Airborne Early Warning (AEW) operations. A combat veteran from Operation Desert Shield and Storm, he also commanded combat deployments for Operation Southern Watch, Operation Enduring and Iraqi Freedom, and conducted continuous 24/7 AEW air patrols after the events of 9/11 for Operation Noble Eagle from Tinker AFB OK. He started his military career in 1985 as part of the Peace Shield Program supporting the RSAF AEW in Riyadh, Saudi Arabia, and completed his final operational tour as Director, Cheyenne Mountain Command Center in 2009. Kevin Mulvihill was awarded a Masters of Public Administration, from the University of Oklahoma, Norman, Oklahoma. His professional education includes graduating from Air Force Fighter Weapons School, Nellis AFB, Las Vegas, Nevada; U.S. Army Command and General Staff College, Fort Leavenworth, Kansas; Air War College, Maxwell AFB, Alabama; Joint Forces Staff College, Norfolk, Virginia; and National Security Studies Seminar 8, Canadian Forces College, Toronto, Ontario Canada, APEX 48 and Harvard Kennedy School for Senior Executives in National and International Security Program (NIS) program.
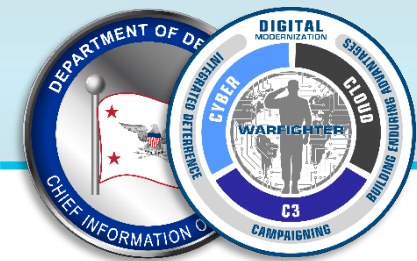
A Call to Industry and Academia

These are ominous days—days whose swift and shocking developments force every neutral nation to look to its defenses in the light of new factors.

- FDR, May 16, 1940

1940: Hitler's threat looms ever larger, with Germany's blitzkrieg across Europe

FDR called to industry. Despite the critics, Ford created the great arsenal of democracy, Willow Run, almost overnight and solved a massive engineering challenge and delivered a moonshot.
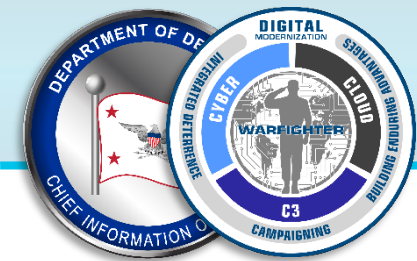
Industry and Academia answered the call to deliver a "Moonshot"
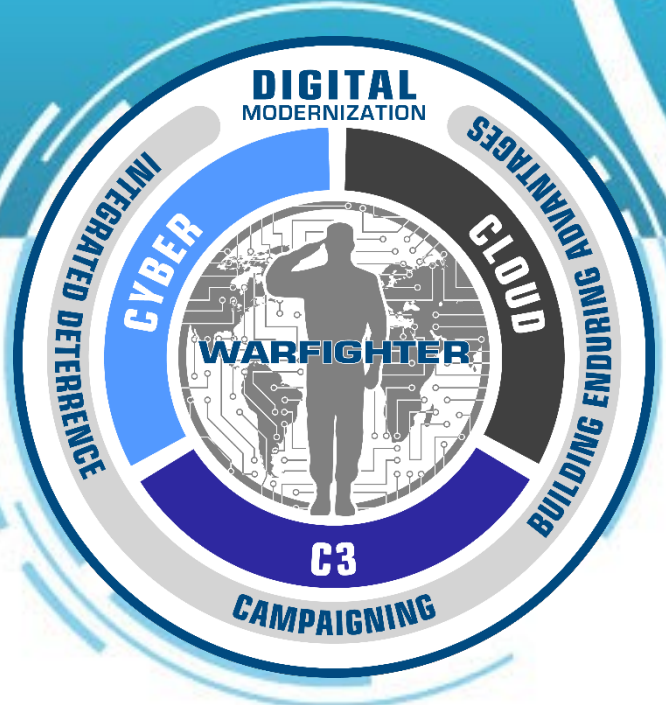
Dynamic Spectrum Sharing (DSS) Framework

DoD CIO, C3, EMSEPP

8 April 2024

Current Environment

Increased Industry Spectrum Needs
- 5G/NextG, IoT, LeoSats; and more
- Connected everywhere at anytime
- **Economic competition with China**

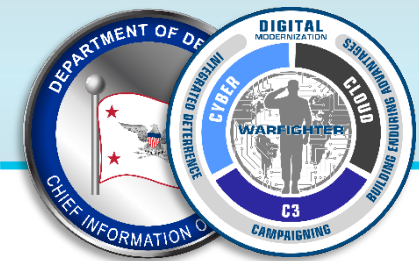### Increased Warfighter Spectrum Needs
- Needs in all domains to support warfighting and mission readiness requirements.

Unrelenting Adversary Actions
- Strategies/actions targeting the United States – including military, economy, and infrastructure
- **Advancing counter-spectrum capabilities**

Spectrum is a STRATEGIC ASSET

Real Threats = Real Spectrum Needs

U.S. Navy warships shooting down Houthi drones in the Red Sea...
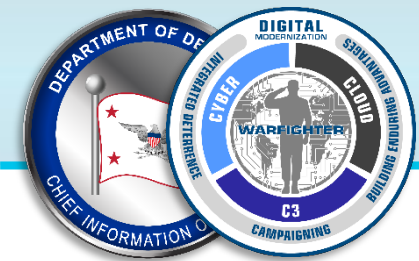

Tracking surveillance balloons from foreign nations...

Multiple other ongoing and emerging threats...

We are living in a "decisive decade"…success is dependent on DoD's assured spectrum access

# Emerging Mid-band Radar Spectrum Sharing (EMBRSS)

- **2021 Infrastructure Investment and Jobs Act (IIJA)** directed DoD to study spectrum sharing with commercial industry in the 3.1-3.45 GHz band

- Critical DoD capabilities rely heavily on the 3.1-3.45 GHz band (land, sea and airborne radar)

- Study found that sharing is **not** feasible at this time, _unless_ certain conditions are proved out, particularly related to **dynamic spectrum sharing at scale**

U.S. Stakeholder

- DoD led (DoD, NTIA, FCC, Industry, Academia)
- 20-month study of 16 priority systems including other federal users (DHS, NASA)
- Over 1,200 pages
- Redacted EMBRSS Report
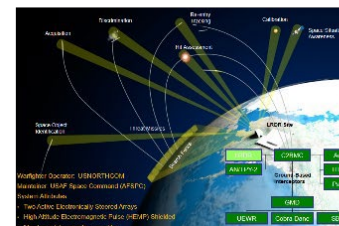
Federal Systems cover the entire United States
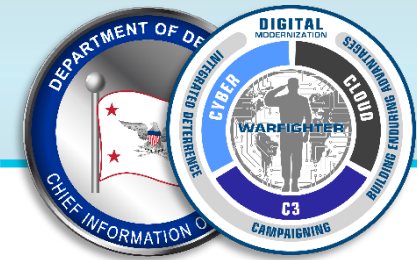
Dynamic Spectrum Sharing (DSS) Framework

Current State: The U.S. Govt does not have a secure, interoperable and integrated DSS framework to support federal and non-federal spectrum access **across** the spectrum

- Current technologies and approaches do not satisfy both DoD and Commercial needs; scaling will be a massive engineering and governance challenge
- Recently completed EMBRSS study identified sharing/co-existence is possible provided key conditions are met
- Pressure for greater spectrum access increases need for a spectrum sharing construct that supports both DoD and the commercial sector

Impact: U.S. Govt's ability to effectively and efficiently coordinate, synchronize and deconflict spectrum access in shared/coexisting frequency bands, from federal operations to commercial access for a myriad of national requirements

National Spectrum Strategy (NSS)
The White House released the National Spectrum Strategy on 13 Nov 2023 to modernize spectrum policy, better manage spectrum, identify bands for study, and establish a "moonshot" DSS effort.
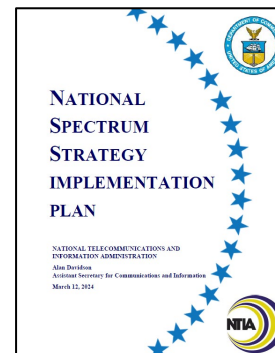
NSS Implementation Plan (IPlan)
NTIA released the National Spectrum Implementation Plan on 12 Mar 24 to provide a public roadmap for the National Spectrum Strategy. *Assigns DoD and NTIA to demonstrate and report on an advanced DSS*

DoD and NTIA are tasked to conduct a 12 to 18-month advanced DSS demonstration and report
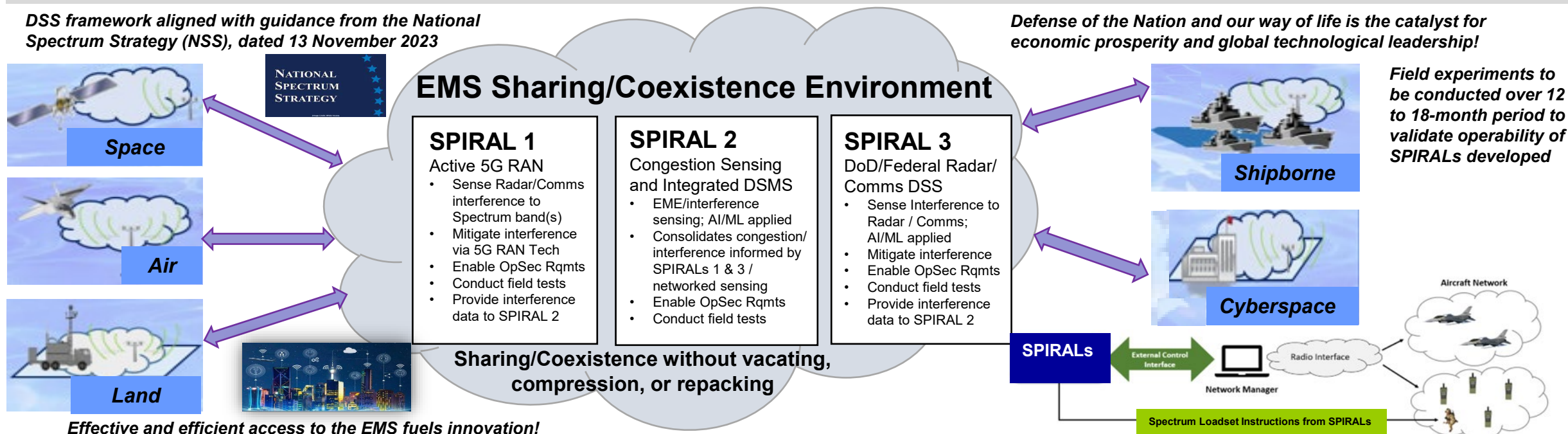
Dynamic Spectrum Sharing - Operational View (OV-1)

Develop Spectrum Sharing/Coexistence based on Science and Data-Driven Processes

The Dynamic Spectrum Sharing (DSS) Framework is an innovative solution to sense the electromagnetic environment, identify congestion and interference among federal and non-federal sources, and enable coexistence within the electromagnetic spectrum.
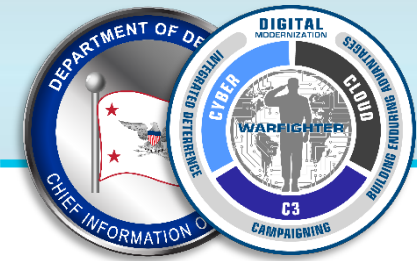
DSS framework aligned with guidance from the National Spectrum Strategy (NSS), dated 13 November 2023

Defense of the Nation and our way of life is the catalyst for economic prosperity and global technological leadership!

Field experiments to be conducted over 12 to 18-month period to validate operability of SPIRALs developed

EMS Sharing/Coexistence Environment

Space

Air

Land

SPIRAL 1

Active 5G RAN
- Sense Radar/Comms interference to Spectrum band(s)
- Mitigate interference via 5G RAN Tech
- Enable OpSec Rqmts
- Conduct field tests
- Provide interference data to SPIRAL 2

SPIRAL 2

Congestion Sensing and Integrated DSMS
- EME/interference sensing; AI/ML applied
- Consolidates congestion/ interference informed by SPIRALs 1 & 3 / networked sensing
- Enable OpSec Rqmts
- Conduct field tests

SPIRAL 3

DoD/Federal Radar/ Comms DSS
- Sense Interference to Radar / Comms; AI/ML applied
- Mitigate interference
- Enable OpSec Rqmts
- Conduct field tests
- Provide interference data to SPIRAL 2

Shipborne

Cyberspace

Sharing/Coexistence without vacating, compression, or repacking

Effective and efficient access to the EMS fuels innovation!

SPIRALs

External Control Interface

Network Manager

Radio Interface

Aircraft Network

Spectrum Loadset Instructions from SPIRALs

EMS Maneuver Space

Congested, Contested, Constrained
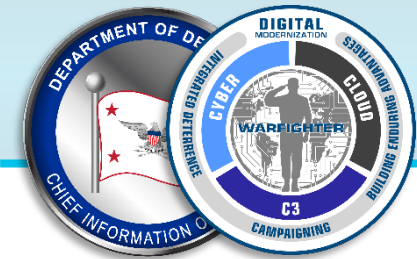
Detect, Exploit, Deny, Disrupt, Destroy

Cyber

Dynamic Spectrum Sharing (DSS) Framework

DoD DSS Framework Definition

Adaptive coexistence within the Electromagnetic Spectrum enabled by evaluation and analysis of current, prescribed, and projected access among spectrum-dependent systems
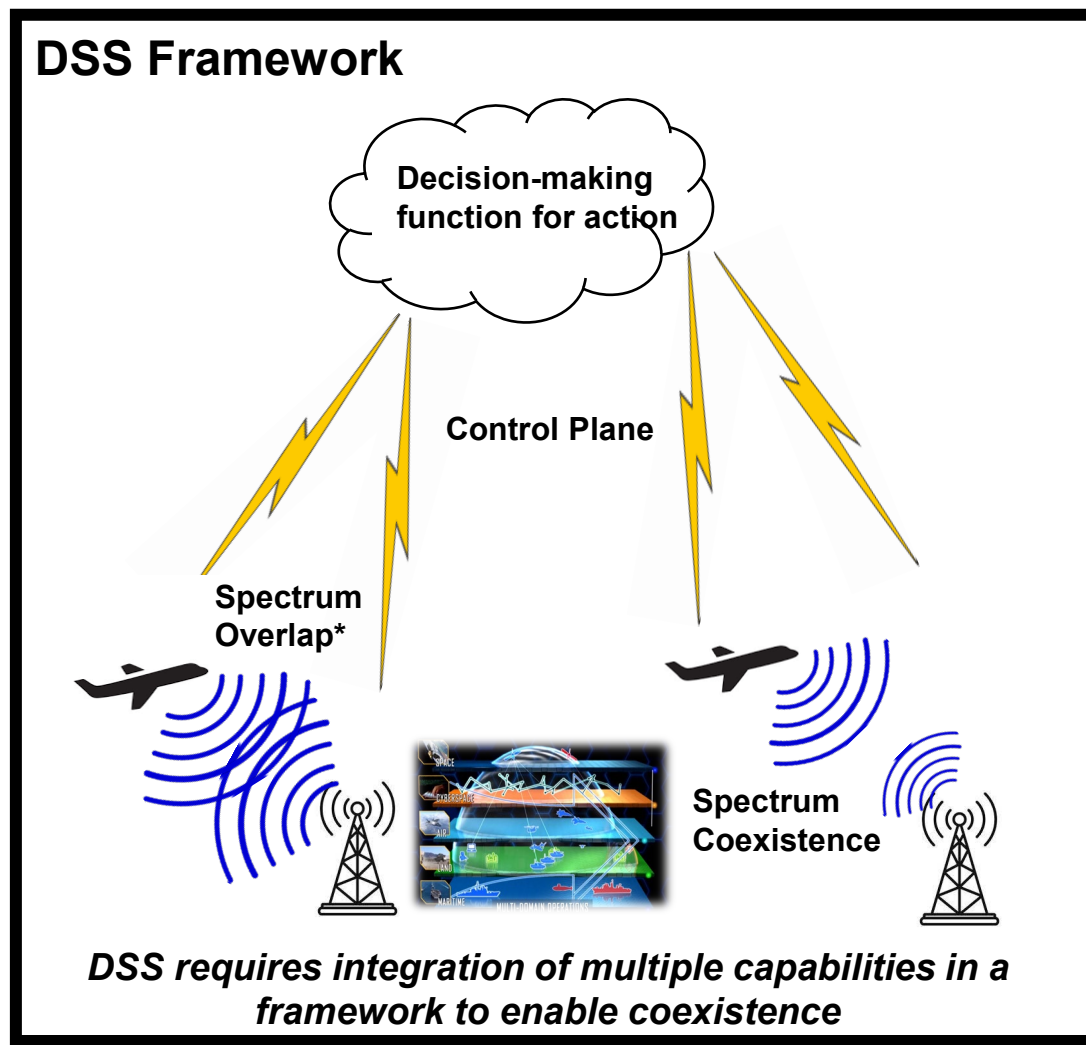
Dynamic Spectrum Sharing (DSS) Framework

- ## DSS Key Technical Elements:

  - Cyber Security
  - Advanced Automation
  - Spectrum Situational Awareness
  - Data-Driven Analytics
  - Dynamically Reconfigurable

  - Operational Security
  - Artificial Intelligence/Machine Learning Capabilities
  - Responsiveness
  - Sensor/Data Informed Deconfliction
  - Modeling & Simulation

DSS requires a sustained Governance Framework, Streamlined Coordination, and Ecosystem Responsiveness to assure coexistence

DSS Framework

Decision-making function for action

Control Plane

Spectrum Overlap*

Spectrum Coexistence

DSS requires integration of multiple capabilities in a framework to enable coexistence

DoD is not interested in controlling commercial terminals

* Spectrum Overlap occurs when all of the spectrum footprint dimensions overlap (time, space, and frequency)
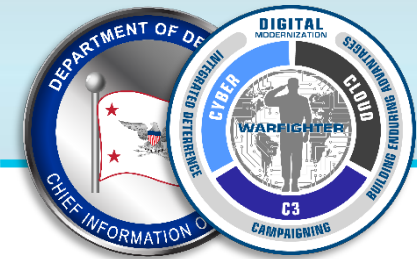
Recent R&D and Experimentation

Resilience
Improving operations in congested Spectrum

- Spectrum Situational Awareness Systems
- Leverage of Non-RF links for data transport
- Spectral Coexistence Solution for Tactical Radios & Ground Radar Systems
- Range Mission Planning & Spectrum Management Tools
- Interference testing between 5G and Aerial radar

Efficiency
Optimizing Spectrum Access

- Large Data Transport Waveform for Ranges
- MIMO for Tactical Radios
- Self-Interference Cancellation
- Same Frequency Simultaneous Transmit and Receive (SF-STAR)

Agility
Increasing flexibility in Spectrum Operations

- Dynamic Spectrum Access (DSA) for Tactical Radios
- RF Interference Cancellation & Mitigation System
- Spectrum Band Aggregation Technologies
- Software-defined radar

Discipline
Intentional control of Spectrum Emissions

- Command & Control Channel for Comms Network Status & Activity
- DSA & Anti-Jam Communication Solution for UAS
- AI/ML-enabled Predictive Spectrum Usage Tool

Over $500M invested in more than 30 projects
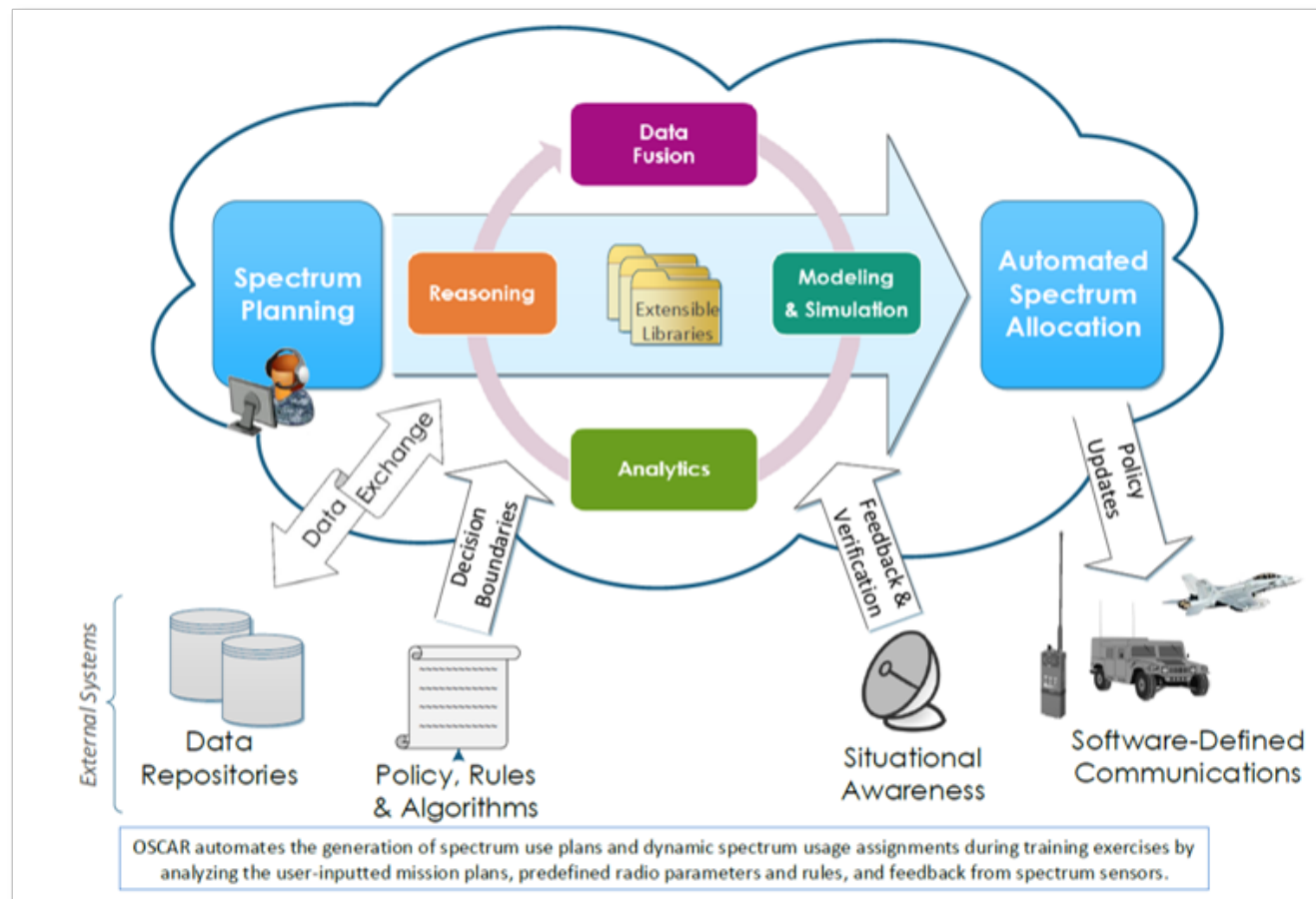
*Not an exhaustive list
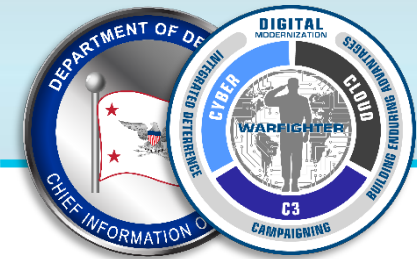
DoD Current Efforts

Complementary efforts are underway within DoD to improve Spectrum Access:

- **OSCAR**: Operational Spectrum Comprehension and Response
- **MICCA**: Multiband Control Channel Architecture
- **RISA**: Risk-Informed Spectrum Access

Integrated Field Testing in FY24

OSCAR automates the generation of spectrum use plans and dynamic spectrum usage assignments during training exercises by analyzing the user-inputted mission plans, predefined radio parameters and rules, and feedback from spectrum sensors.

Collaboration to achieve coexistence is a DoD priority

Stakeholder Input to DSS Framework

DoD cannot fulfill a Dynamic Spectrum Sharing Framework without our partners; initial focus is on 3.1 - 3.45 GHz
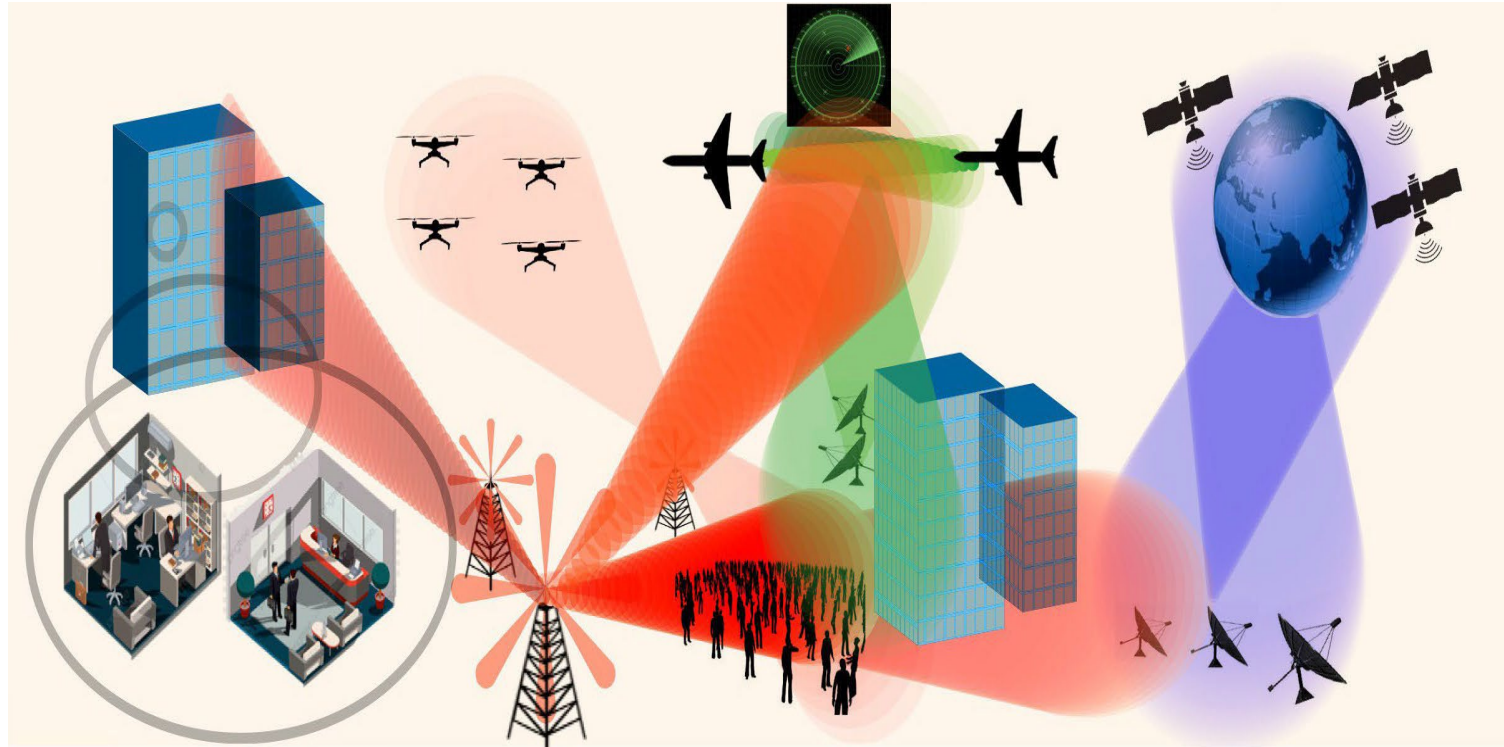
DoD welcomes input to help align further sharing/coexistence opportunities
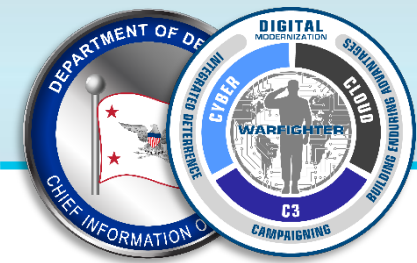
Strategic Way Forward

Actions:

- **Rigorous assessment of technical, and policy conditions**

  - Establish a dynamic spectrum sharing (DSS) framework

- **Develop a DSS Pilot platform** that enables a whole of nation way forward to improve management of the nation's airwaves

- **Continued partnership with industry**

  - Further the trust and transparency built in PATHSS

  - Support validation of nine conditions and awareness of advances in technologies

- **Remain attuned to advances in spectrum technologies**

  - <u>Today's</u> formidable sharing challenges may be *solved* by <u>future</u> tech

Necessities:

- **DoD, DIB, Academia, and Comm industry** expertise to assist with current solution identification

- **Joint and Service SMEs** for ops/risk/cybersecurity assessments

- **Access** to DoD **test, training, and exercise** venues

- Conduct **table-top exercises** in **partnership** with **industry** and other **stakeholders**

- **Follow-on consortium** driving trust, transparency, and policy change

- **Stakeholder** collaboration on a whole of nation dynamic spectrum sharing framework

We call on you again!
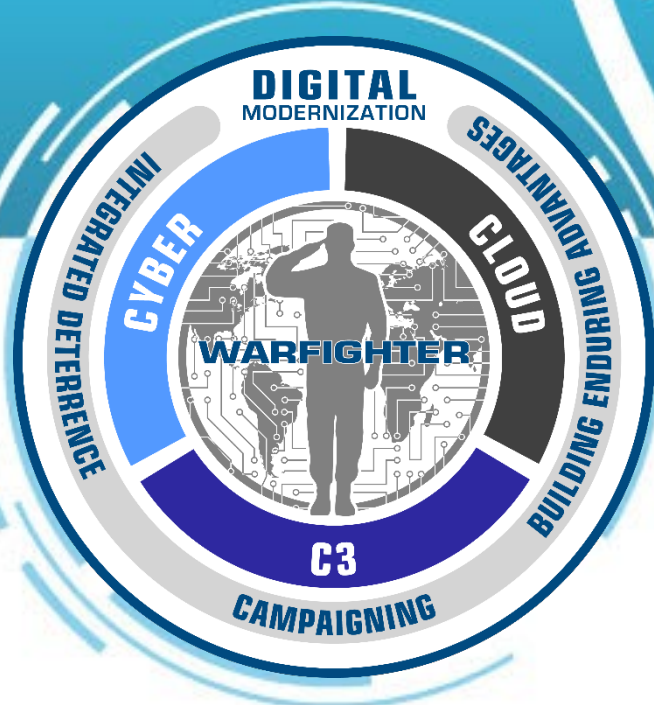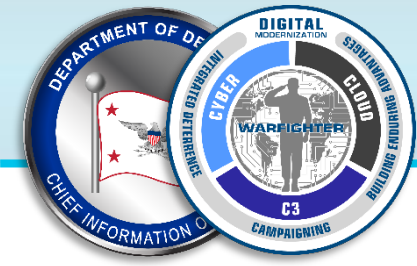
Agenda

Welcome

- Ms. Meredith Attwell Baker (CTIA)
- Hon. Sherman (DoD CIO)
- Lt. Gen. Isaacson (JSJ6)

Break – 15 Min

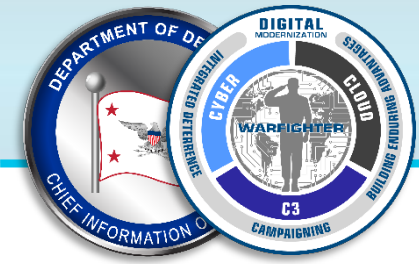Dynamic Spectrum Sharing (DSS) Framework

- Mr. Matthew Pearl (EOP/NSC)
- Mr. Kevin Mulvihill (DoD CIO C3)
- Dynamic Spectrum Sharing (DSS) Framework

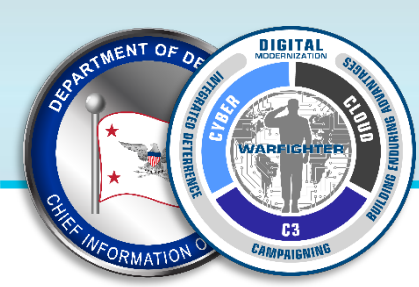National Spectrum Consortium (NSC) & PATHSS Overview
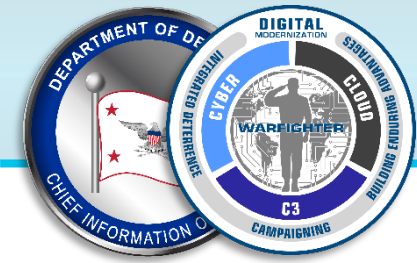
- NSC Overview
- PATHSS

Next Steps

Questions

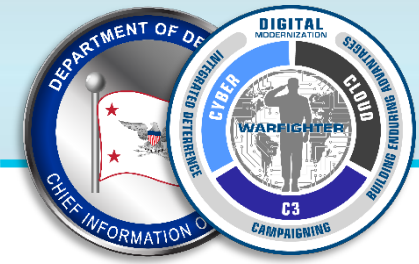# National Spectrum Consortium (NSC) Overview

PATHSS Overview

PATHSS Objective

- Primary objective is to continue to build **TRUST** and **TRANSPARENCY** between industry and DoD through:
  - A transparent process with the broadest possible involvement in PATHSS, with expanded access to information (Proprietary and Controlled Unclassified Information (CUI))
  - A process to share proprietary and classified information
  - Demonstrated, sustained engagement by DoD leadership

DoD/NTIA PATHSS Organizational Structure
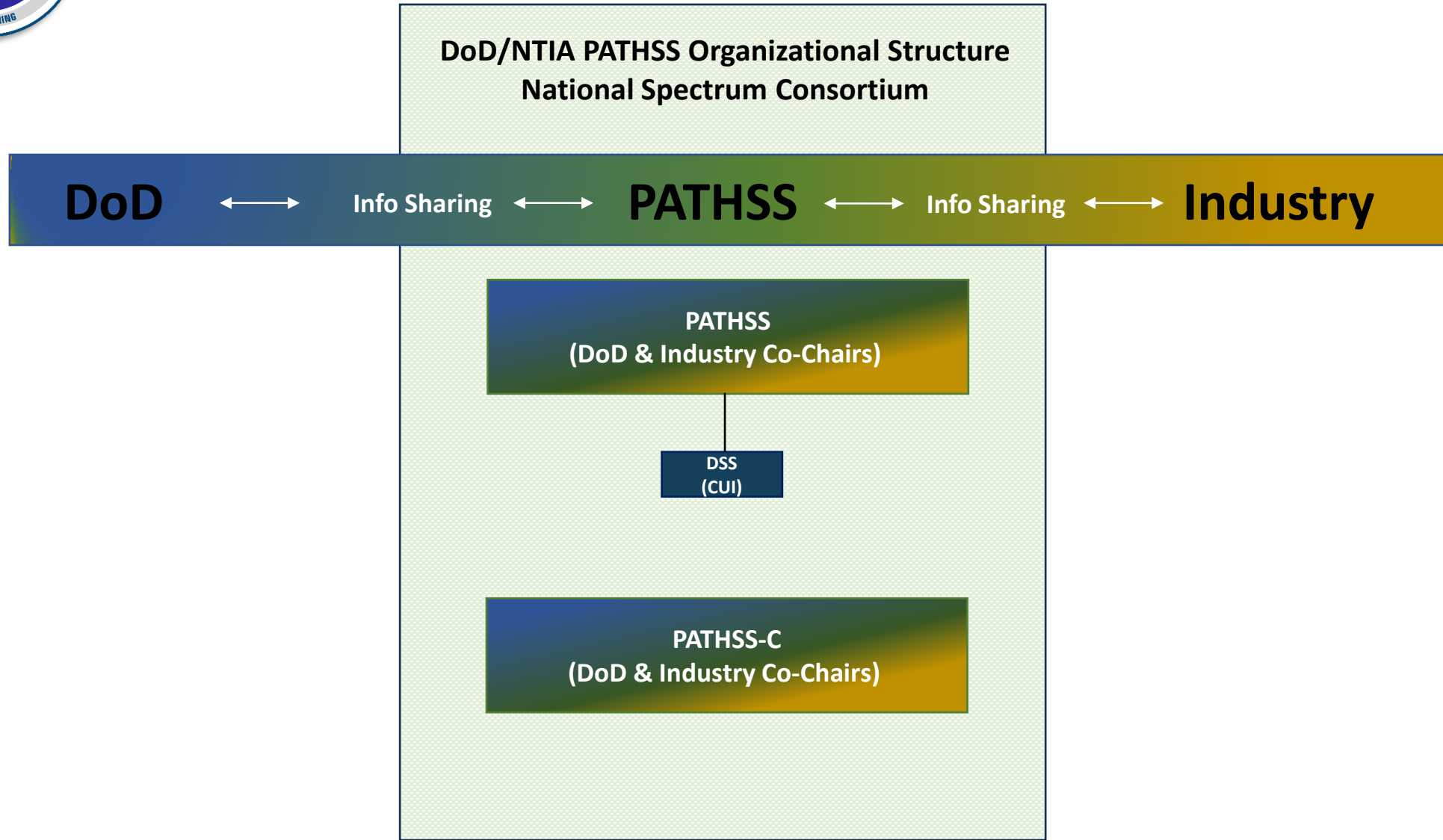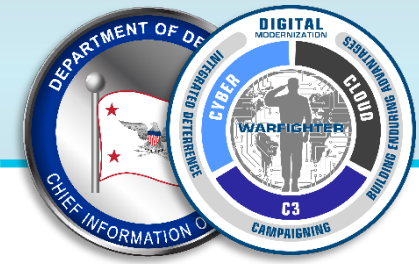
Next Steps

- PATHSS Meeting – 22 May 2024 (T)

Questions?