U.S. Army Signal School

Leader - Teammate - Communicator

Office Chief of Signal (OCOS) Proponent Update

Augusta TechNet 2021

18 August 2021

Agenda

- CMF 25 Military Occupational Specialty (MOS) Convergence
- Warrant Officer Update
- Data workforce

MOS Convergence

MOS Convergence Background

- Career Management Field (CMF) 25 not structured to meet to enable mission command in an expeditionary, multi-domain, full spectrum, and large scale combat operational environment.

- Convergence of CMF 25 from its current 17 MOS structure to 7 focus-oriented MOSs, supports the Signal Regiment's efforts to create an enlisted force that is multi-disciplined and optimally trained.

- ***MOS decisions influenced by a CSM/SGM panel and two SME panels with extensive technical knowledge and operational experience.***

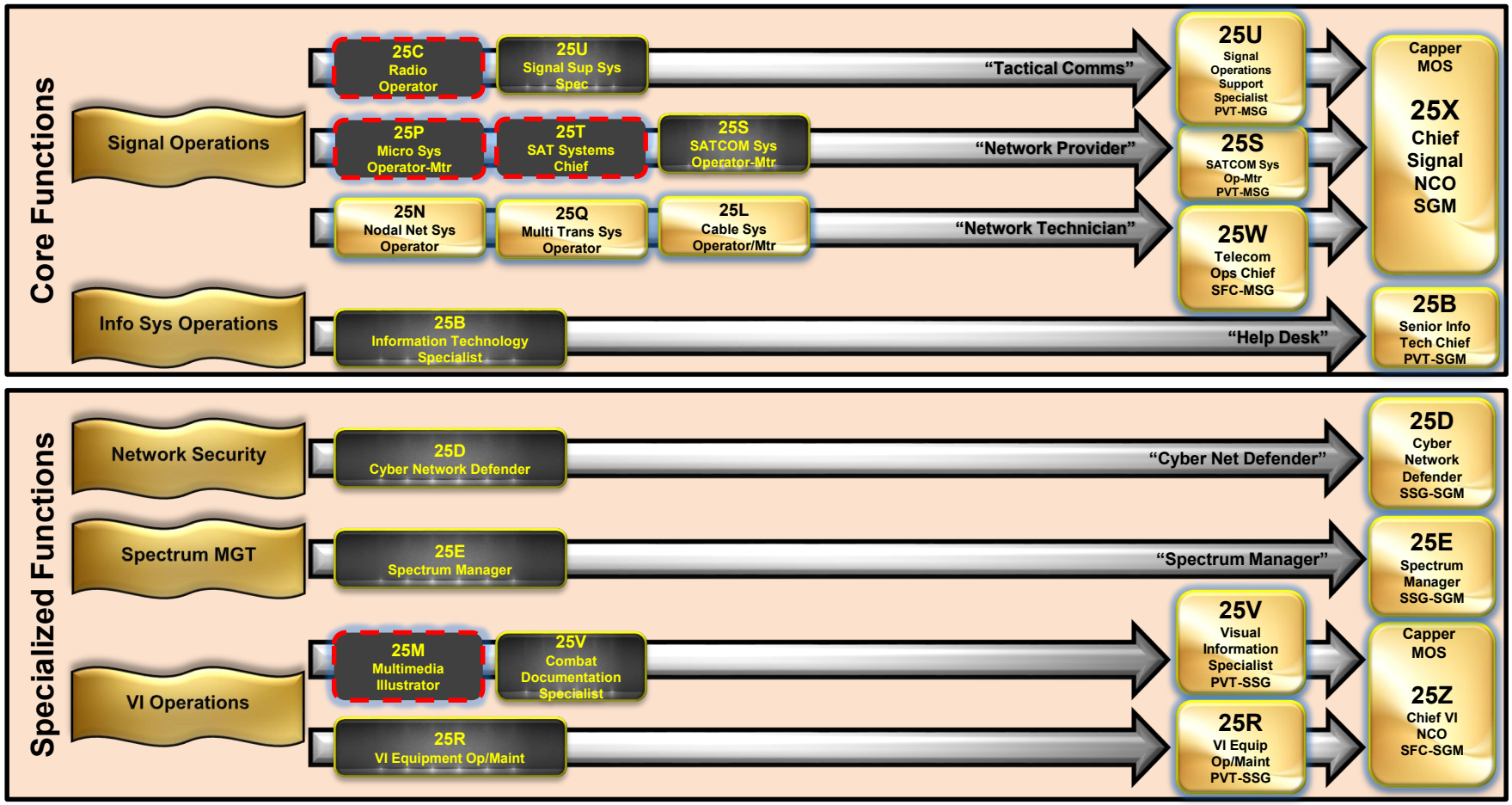
- MOS convergence created an opportunity to synchronize DA mandated enlisted grade plate reductions with emerging force structure. Provided an integrated DOTMLPF solution that drove adjustments linked to the institutional Army to create/merge/adjust GCDM within CMF 25 and balance at the MOS level.

- The Signal School reviewed its 17 enlisted MOSs and developed an extensive, multi-phased MOS convergence strategy that
  - ✓ Alleviates MOS task redundancy,
  - ✓ Eliminates NCO “capper” MOSs that merge multiple MOSs at the senior NCO level, and
  - ✓ Rebalances CMF 25 to fall within approved GCDM levels.

HQDA EXORD 048-18 STRUCTURE AND PERSONNEL FRICTION dtd 3 January 2018 directed MOS consolidations where possible; FRAGO 2 directed a grade plate review.

Phase 1 Signal Enlisted MOS Convergence

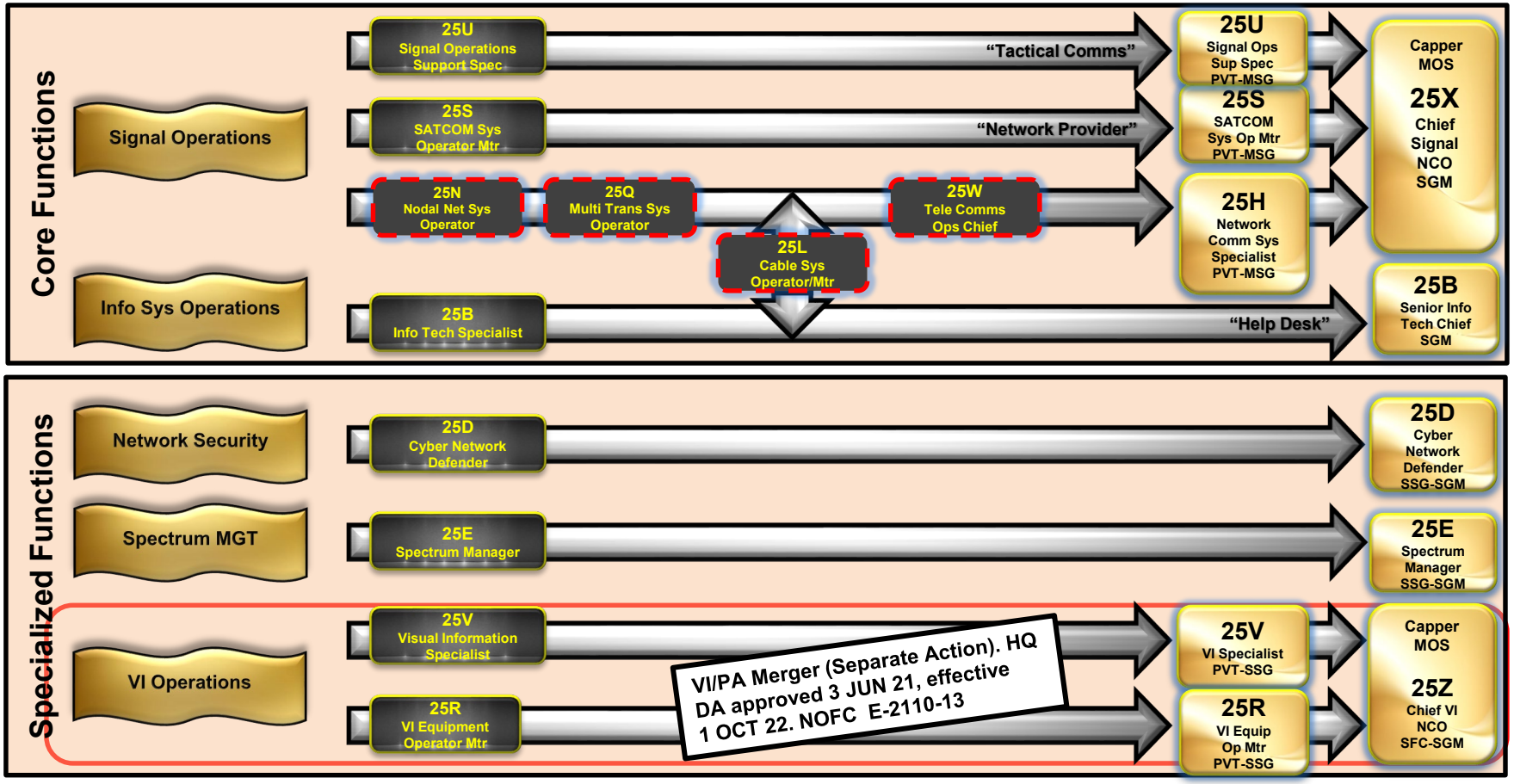
Approved 3 OCT 2019; effective 1 OCT 2021



Reduces CMF 25 MOSs from 17 to 13

Phase 2 Signal Enlisted MOS Convergence

Approved 14 July 2021; effective date: 1 OCT 2022



Revised
Deleted
MOSs
Merge

Reduces CMF 25 MOSs from 13 to 7

Warrant Officer Update

255S - Information Protection Technician

CURRENT

Information Protection Technician

Subject matter experts on integrated cybersecurity activities and capabilities within the Army's portion of the cyberspace domain on the Department of Defense Information Networks (DODIN). They are responsible for:

- ❑ Designing, building, configuring, operating, maintaining, and protecting cybersecurity activities and capabilities in support of internal defensive measures within the DODIN to locate threats and respond to unauthorized activity, security alerts, and threat information enabling mission command.
- ❑ Oversee the implementation of cybersecurity policies, directed internal defensive measures, cryptographic network (cryptonet) planning, Electromagnetic Spectrum Operations (EMSO) to achieve electronic protect, and electronic key management required to support secure communications.
- ❑ Train and supervise cybersecurity personnel in the building, configuring, securing, defending, protecting, and sustaining cybersecurity equipment to maintain an assured network environment enabling combat power projection.
- ❑ Provide technical guidance and advice to commanders and staffs on the management and operation of Army, Joint, intergovernmental, interagency, and multinational cybersecurity efforts to include the identification of mission critical networks and systems while operating within optimal, degraded, intermittent, or latent environments

PROPOSED

Cyberspace Defense Warrant Officer

Subject matter experts on integrated cyberspace defensive operations activities and capabilities within the Army's portion of the cyberspace domain within the Department of Defense Information Networks (DODIN). They are responsible for:

- ❑ Collecting, analyzing, interrogating, and dissecting data and information in order to enumerate, illuminate, locate, eradicate threats and respond to unauthorized activity, security alerts, attempted exploitation, data exfiltration, escalation, and any additional threats to Army operations and mission command.
- ❑ Oversee the implementation of cybersecurity and cyberspace defense policies at all echelons.
- ❑ Direct internal defensive measures across the integrated enterprise and tactical network, assist in cryptographic network planning and support cyber electromagnetic spectrum operations (CEMA) to reduce detection by electronic signature.
- ❑ Train and supervise cybersecurity and cyberspace defense personnel in the building, configuring, operating, securing, defending, protecting, and sustaining cybersecurity systems and software to maintain a protected network environment thus enabling combat power projection in all warfighting domains.
- ❑ Provide technical guidance and advise Commanders and staffs on the management and operation of Army, Joint, intergovernmental, interagency, and multinational cyberspace defense efforts to include the identification of key terrain, mission critical networks, nodes, applications and systems while operating within optimal, degraded, intermittent, or latent environments.

- Source: SC DA PAM 600-3 Smartbook

Warrant Officer MOS 255S Update

January 2022 — First "official" 255S WOBC scheduled.

October 2021 — MOCS action to revise MOS 255S from a CW3-CW4 force structure to a CW2-CW4 force structure takes effect 1 October 2021.

We Are Here

September 2021 — Third 255S accessions (recruiting) board.

May 2021 — Second 255S accessions (recruiting) board. 8 out of 8 selected.

April 2021 — MOCS submitted to change 255S from "Information Protection Technician" to "Cyberspace Defense Warrant Officer" for implementation in FY24.

January 2021 — First 255S accessions (recruiting) board. FY21 accessions quota is 24. 8 out of 8 selected.

January 2021 — Second 255S WOBC Pilot course: 18 WO1s (6 AD, 6 NG, 6 AR). All 18 Warrants successfully graduated.

June 2020 — MOCS action to revise MOS 255S from a CW3-CW4 force structure to a CW2-CW4 force structure is approved with an effective date of 1 October 2021. This includes the establishment of MOS 255S Warrant Officer Basic Course.

January 2020 — First 255S WOBC Pilot Course: 12 WO1s (6 AD, 4 NG, 2 AR) that met specific perquisites participated in the 21 week long resident course. All 12 Warrants successfully graduated.

2019 — Decision made to revise 255S to W2 – W4 structure. Zero growth initiative drove realignment of all MOS WOAC and WOBC to create 255S WOBC. Each WOBC is 21 weeks and each WOAC is 12 weeks.

MOS 255S Career Map

255S (AC) Warrant Officer Professional Development Model

WO YRS SVC	0	2	4	6	7	9	11	12	16	17
Promotion Boards	WO1	CW2		CW3 BOARD	CW3		CW4 BOARD	CW4	CW5 BOARD	
	COMPANY GRADE WARRANT OFFICER				FIELD GRADE WARRANT OFFICER					

Institutional				
PME	**WOBC**	**WOAC**	**WOILE + SWOILE**	**WOSSE**
Functional	• Airborne/Air Assault/ Ranger	• Airborne/Air Assault/ Ranger • Cyber Operations Planner Course (COPC)	• Joint C4 Planners Course • Mission CMD Digital Master Gunner	• How the Army Runs
Operational				
Key Developmental Assignments				
	• Brigade Combat Team (BCT) • Cyber Warfare Support Battalion • Multi-Functional Support Brigade • Security Forces Assistant Brigade • Functional Support Brigade	• Brigade Combat Team (BCT) • Cyber Warfare Support Battalion • Multi-Functional Support Brigade • Security Forces Assistant Brigade • Functional Support Brigade	• 2nd IO Command • DIV G6 • MI BDE/ CSB • Multi-Domain Task Force • Regional Cyber Center • WHCA/JMC	• ASCC/Joint/Corps • Strategic Sig Bde • Theater Sig Cmd • DISA/WHCA • Futures CMD Staff • Regional Cyber Center
Broadening Assignments				
		• TAC Officer, WOCC	• Jr SC WO Career Manager • Instructor, Signal School • TAC Officer, WOCC • O/C, CTC • Doctrine Writer, CCOE • Training with Industry (TWI) • Advanced Civilian Schooling (ACS) • Signal Branch Fellowships	• Sr SC WO Career Manager • HQDA Staff • Instructor, WOCC • Capabilities Developer, CCOE • CDR, 1st WOC • Training with Industry (TWI) • Advanced Civilian Schooling (ACS) • Signal Branch Fellowships
Self-Development				
Academic (Army Skillport | FedVTE | WOPD | Civilian IT Conferences | AFCEA Seminars I TechNet)				
	• ASSOCIATE degree in STEM discipline	• ASSOCIATE degree in STEM discipline	• UNDERGRADUATE degree in STEM discipline	• GRADUATE degree in STEM discipline
Credentialing				
	• CompTia (CySA, CASP+) • Microsoft (Cloud Security) • SANS (GCDA, GCLD, GSOC)	• Microsoft (Cloud Security) • SANS (GCDA, GCLD, GSOC, GPYC)	• CISSP • PMP • SANS (GNFA, GCFE, GCFA, GPEN)	• CISSP • PMP • SANS (GNFA, GCFE, GCFA, GPEN)

Data Workforce

Building a Data Workforce

Implementing flexible and adaptable training to meet current and future requirements.

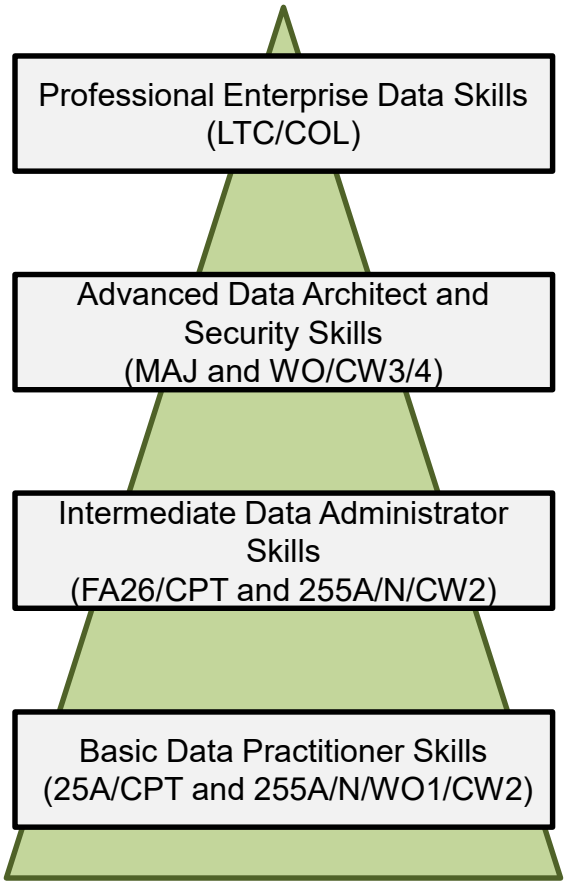
What must we be able to do:

- Build infrastructure and architecture for data generation
- Clean and wrangle data into a usable state
- Produce readiness and curation of data: efficiency, scaling, resilience, security, interoperability, formats, and more
- Build and maintain the organization's data pipeline systems

Data Skill Requirements

- Database System Design and Maintenance
- Data Manipulation and Visualization
- Programming (CS/ MIS foundation)
- Extract Transform and Load (ETL)
- Cloud Fundamentals
- Data Analysis

Data Skill Levels



Actions

- ❑ Leverage ACS PhD Programs
- ❑ Develop flexible and adaptable educational and training opportunities for Warrant Officer
- ❑ Leverage ACS and TWI programs
- ❑ Add intermediate data engineering education to FA26A/B and 255A/N WOAC
- ❑ Add foundational data education at SCCC and 255A/N WOBC

Developing Data skills at echelon throughout the Signal Regiment

Signal Regiment Data Workforce Operational Planning Team

Purpose: To develop a strategy for the Signal Regiment to posture itself to support emerging data requirements across the Army and support the larger DOD strategic effort to build, man and train the data workforce in support of Multi-domain operations.

(IAW HQDA EXORD 009-20 Army Data Plan Implementation).

LOE 1: What's in A Name? – Review current duty titles and descriptions at echelon of FA26 and Warrant Officer MOSs to align more accurately with Cyber/Data Work Roles as defined in Defense Cyber Workforce Framework and DODD 8140.1

- **1.1** - Crosswalk and validate current duty responsibilities with DODD 8140.1 work roles
- **1.2** - Better articulate roles and responsibilities for Signal personnel across the force at echelon using more accurate naming convention
- **1.3** – Communicate/survey the force on the change in identity

End State: Submit Military Occupational Classification and Structure (MOCS) documentation NLT June 2021 to changes in personnel requirements, authorizations and training in manning documents that impact the Signal Regiment for implementation in FY24.

LOE 2: Force Structure - Identify personnel billets with in the Signal force structure that could potentially be reallocated at echelon to better support emerging data requirements

- **2.1** - Internal focus on Signal force structure to reallocate personnel to enhance capability at echelon.
- **2.2** – Determine if structure changes are required at strategic and tactical echelons.
- **2.3** - Review of WO and FA26 positions in non-Signal organizations left over from legacy systems no longer used or do not require specialized IT training to operate and maintain

End State: Approved force structure change to include a specified data centric organization at echelon for implementation for Total Army Analysis (TAA) 26-30

LOE 3: Train The Force – Incorporating data and cloud technology training into existing PME and surge capability into the work force by utilizing ACS, TWI, and Direct Commissioning

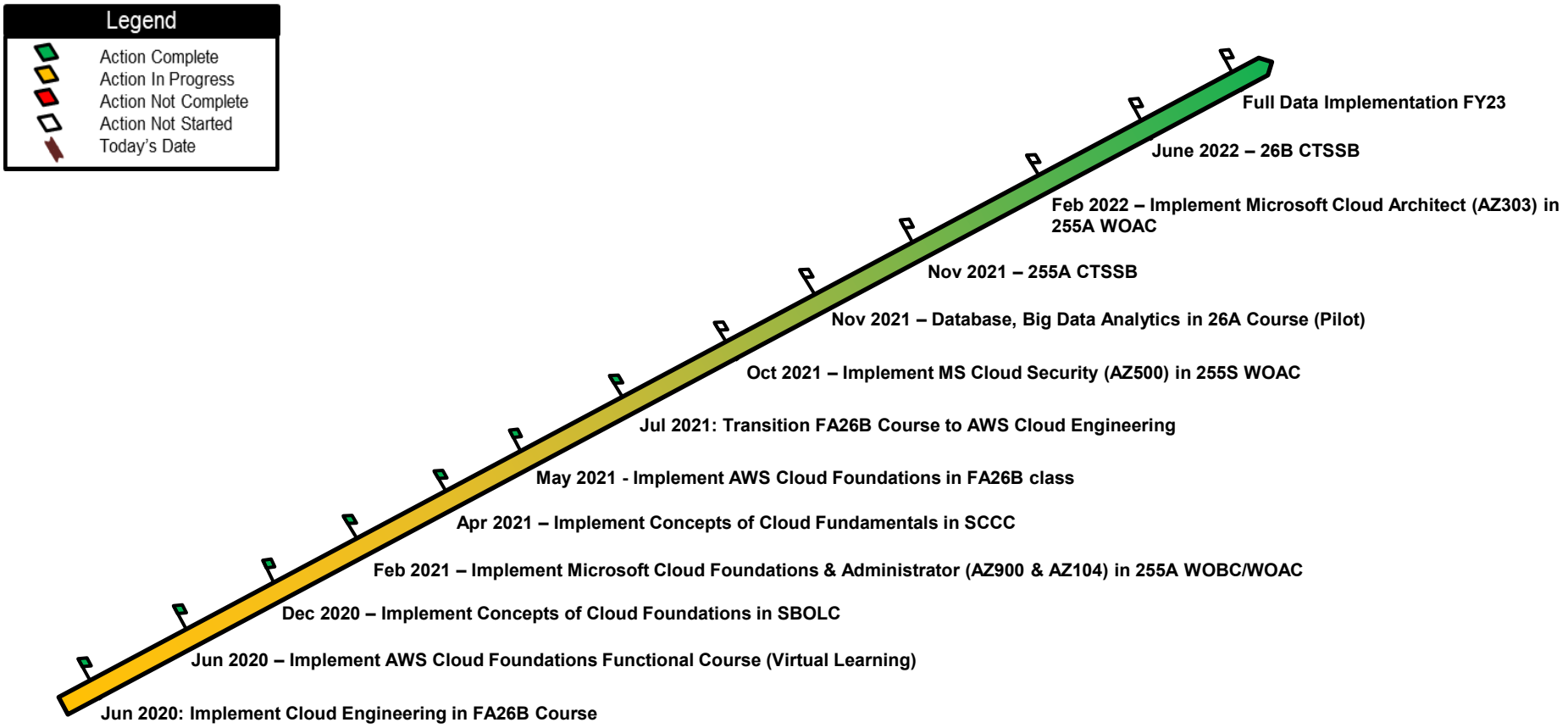
- **3.1** - Pilot program for training of cloud platforms in 255A and 26B Courses
- **3.2** - Incorporate Data/Cloud Foundation Training in other branch IET and PME courses
- **3.3** - Incorporate Data/Cloud Training in select ALC/SLC Courses
- **3.4** - Identify and code position in the force through AERS for Data Trained Workforce
- **3.5** - Crosswalk specific training and education requirements over a career lifecycle

End State: Fully resourced Programs of Instruction for applicable resident courses and virtual learning paths for continuous education.

2028

A modern, data-centric workforce ready to execute data management and governance across the enterprise in support of multi-domain operations.

Training Implementation Timeline



Current Curriculum

- Scripting Language Familiarization (FA26A)
- Conduct Auto Scaling/Load Balancing (FA26A)
- Programming for Network Engineers (FA26A)
- Network Programming (FA26A)
- Quality of Service (255N WOBC/WOAC)
- Network Programming (255N WOBC/WOAC)
- Scripting Language –Powershell (255A WOBC)
- Scripting Language –Python (255S WOBC/WOAC)
- Concepts of Cloud Fundamentals –Juniper (FA26B)
- Cloud Engineering –Juniper (FA26B)
- Scripting Language Familiarization (FA26B)
- Basics of Software Defined Networking –Juniper (FA26B)
- Network Programming & Automation –Juniper (FA26B)
- Intrusion Analysis (25D30)
- Incident Handling (25D30)
- Enterprise Defense (25D30)
- Database
- Intro to Data Science & Big Data
- Understanding the Big Data Framework
- Big Data Tools and Concepts
- Big Data Analytics, ETL & Intro to R
- Analyzing Data through R
- Big Data Solution Engineering
- Social Media, Mobile Analytics, and Visualization
- Understanding Machine Learning
- Essentials of Python

Discussion