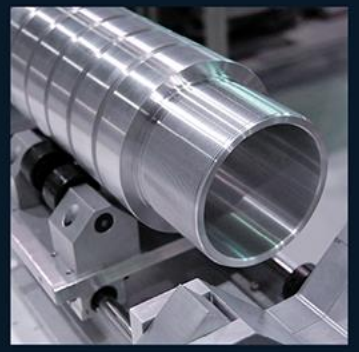
NCDMM

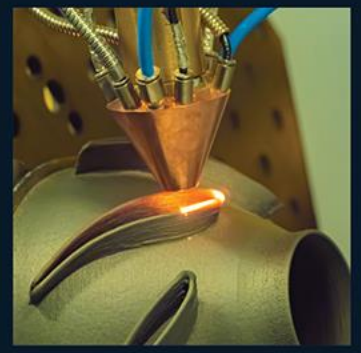
NEVER A FAIR FIGHT








ncdmm.info@ncdmm.org

AMIP (Advanced Manufacturing Intelligence Platform)

NCDMM

Supporting Army readiness through a robust digital additive manufacturing supply chain

AMNOW

Joe Veranese
NCDMM
Vice President & CIO
Joe.Veranese@ncdmm.org

AMIP (Advanced Manufacturing Intelligence Platform)

Where does AMNOW fit in the Digital Thread?

AMIP (Advanced Manufacturing Intelligence Platform)

NCDMM

Demonstrating a robust and capable digital additive manufacturing supply chain supporting Army readiness

Elevating the capabilities of the additive manufacturing supply chain

- Technology, materials, service
- Supporting processes
- Cybersecurity
- “Low barrier of entry”

Elevating the additive manufacturing process as a robust, reliable technology

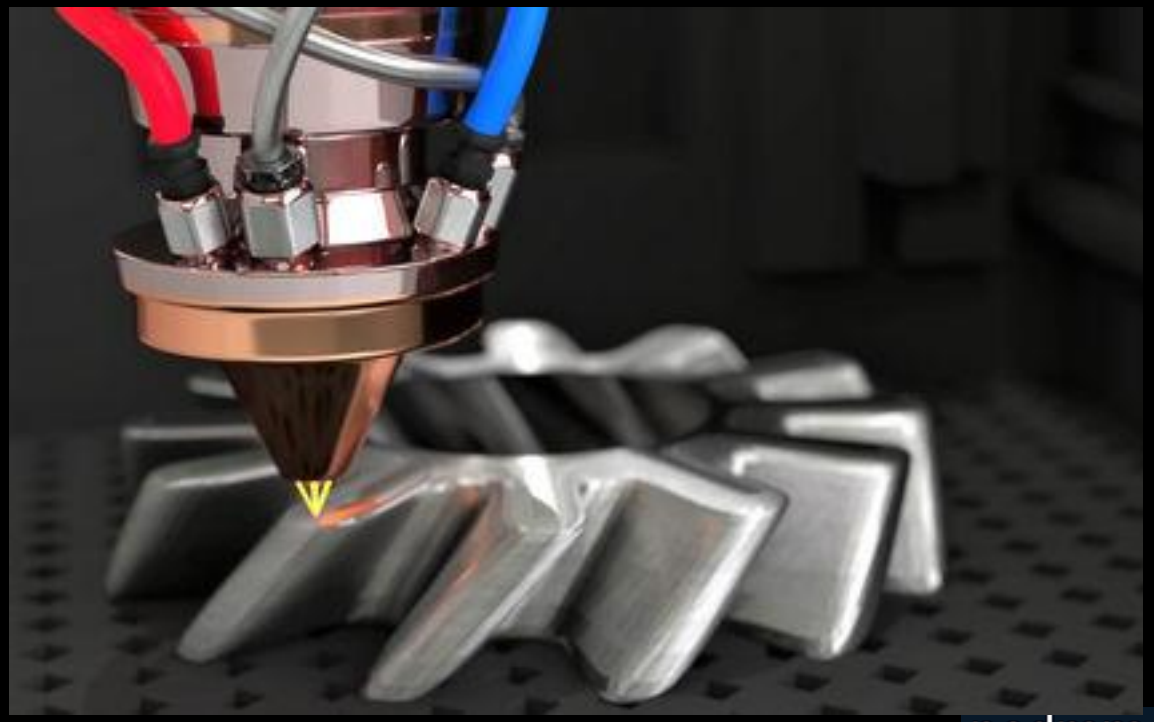
- Complex parts
- Difficult-to-source parts & components
- Process monitoring
- “Sharpest tool”

Visualizing the additive manufacturing process & supply chain back to US Army

- Regional focus with national scale
- Easy access to this capable technology & the supply chain
- “Source with confidence”

How is AMNOW Accomplishing the Goals

Identify Army Relevant Parts → Source Through the Supply Chain → Monitor Production Processes → Add Production Data to Army Digital Thread → Deliver Parts and Align Production Process Data → ~Analytics~



AMIP
Advanced Manufacturing Intelligence Platform

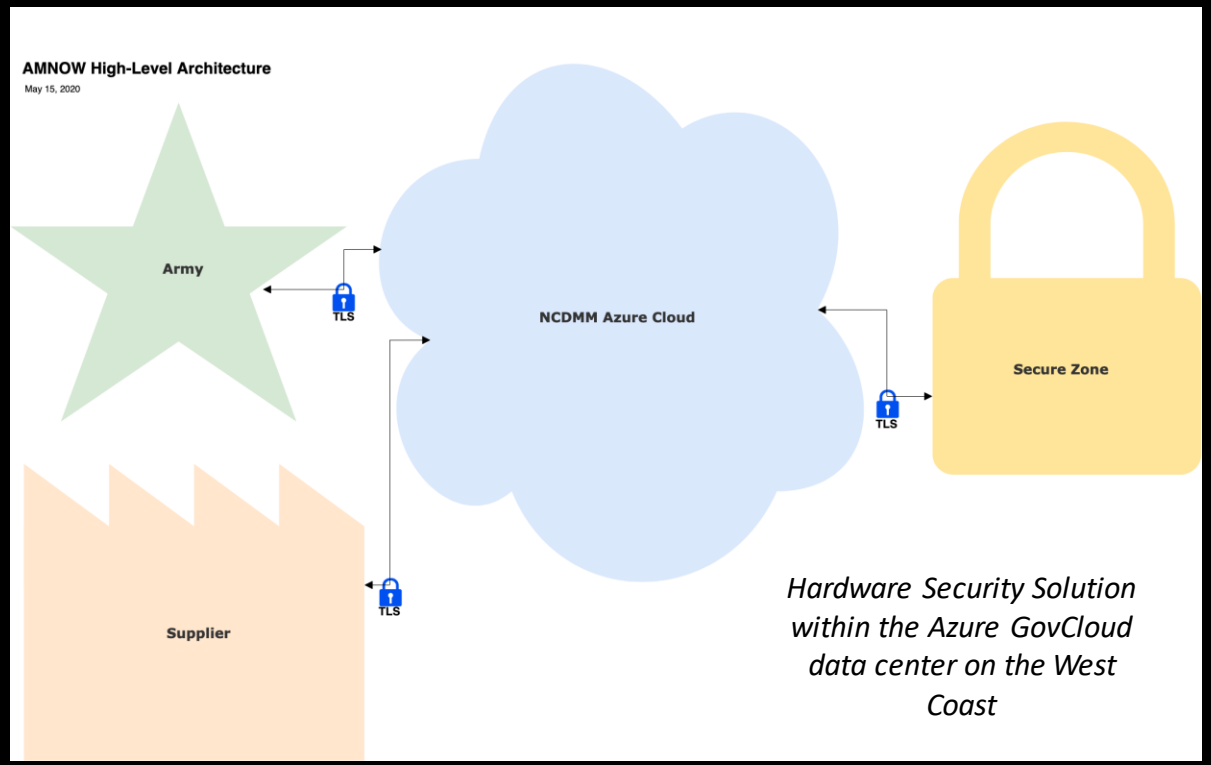
- The AMIP system was developed to improve speed by consolidating and automating various Additive Manufacturing Processes and workflows.

- AMIP shortens production timelines by streamlining the manufacturer selection and bidding process.

- AMIP provides a higher degree of confidence to the customer by automatically tracking production build details. Ensuring that process stage gate requirements were met.
  - This incentivizes manufacturers to improve quality.
  - And allows customers to analyze and compare parts quality across manufacturers and manufacturing process types.

AMNOW – GCC (Government Commercial Cloud)

The AMNOW program has established a secure data repository in Azure GCC to facilitate its demonstration of the AMIP capabilities



The AMNOW cloud space is representative of a typical existing Army data repository with over 19 Army relevant Technical Data Packages

- AMIP digitally interrogates Army TDPs to extract process relevant information as a basis for establishing the sourcing tasks
- AMIP allows manual entry and deletion of process requirements that were derived from the initial TDP interrogation
- AMIP securely transmits all required data and information associated with the solicitation and bidding process from the Secure Zone to Suppliers including TDPs, SOWs, part specifications, process specifications and material specifications
- AMIP secures all information sent to and from the cloud

AMIP and Connection to the Supply Chain

AMIP can gather build and QA information through LIMS (Learning Integrated Manufacturing System) Devices. These can track data from any sensor regarding environmental conditions, build processes, post-production, or QA testing. This data can be aggregated and analyzed in a myriad of ways.

- Predefined and expandable list of KPI's to track.
- Allows for direct sensor expansion.
  - No limit to the number of sensors and metrics that can be tracked.
- No ongoing license costs.
- Connectivity with over 50 language protocols.
- Demonstrated Capability (20 years).
- User friendly, configurable Dashboards.
- Manual Data entry if needed.
- COTS components.
- Does not require cloud connectivity (Supports Air Gap).

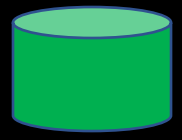
AMIP
Tokenization & Encryption of Data

The AMNOW program offers a way for SMMs to connect to the digital supply chain while still protecting sensitive information

Raw Data from IIoT System
One of 3 Paths Determined by Attributes Set by Supplier

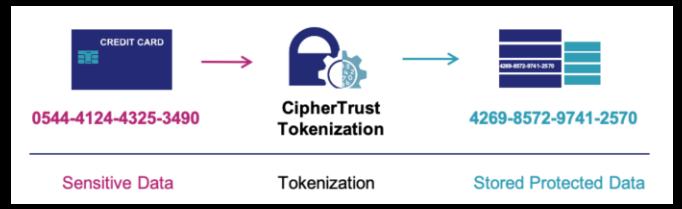
Non-Sensitive

Only AMIP Users Can Use

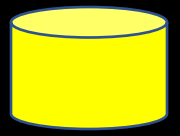


Non-Tokenized Data Sent

Sensitive



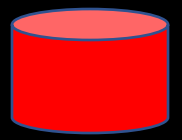
Only AMIP Apps Can Use



Only Tokenized Data Sent

Prohibited

Actual Data Not Sent



Only Data Identifiers Sent

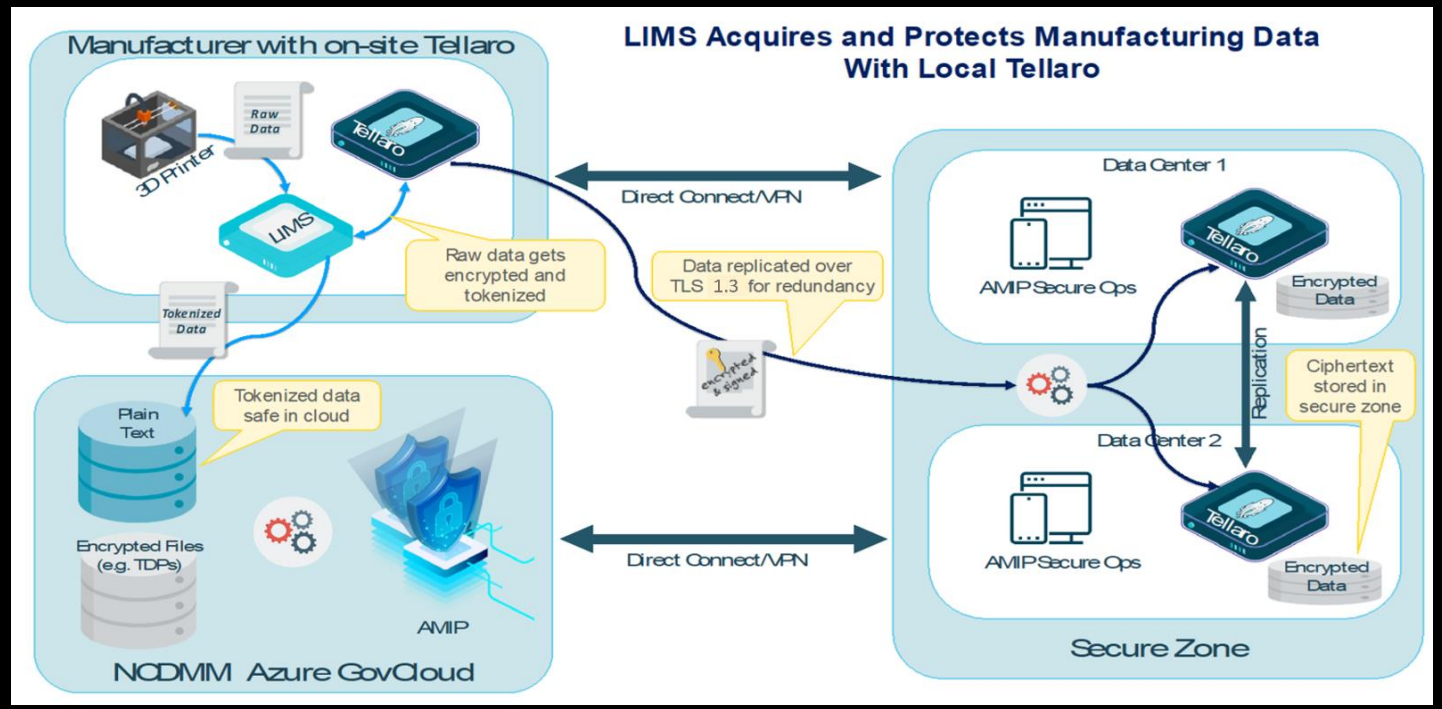
All Data is Encrypted Prior to Sending
Regardless of its Attribute Selection

- Standards based IIoT Edge Devices purchased and controlled by the supplier set the data attributes via its user interface to identify sensitive information
- Standards based IIoT Edge Devices call a local tokenization routine to convert sensitive data to tokenized data
- Data deemed so sensitive it cannot be exposed outside the Supplier's domain is not sent and instead a supplier specified data identifier is provided to the cloud
- Buyer specifies data retention duration via contract requirement for data not sent to cloud and uses the data identifier to initiate access to information if needed

AMIP Security (Data Encryption/StrongKey)

FIPS 140-2 certified encryption in the cloud is used for additional protection of sensitive data as part of AMIP's layered defense strategy. The cloud environment has established a Secure Zone enabled by a cluster of StrongKey devices collocated within an Azure GCC data center. Data can be tokenized with the token now carrying none of the identifying information of the original data. The tokens are stored on a physically separate space in the secure zone. In the event of a breach, any stolen data is worthless. As an example: Someone's PII might have medical records, but this is just worthless medical information without knowing who it is associated with. The name, address, phone number etc. is hidden and locked in the tokens.

- AMIP Architecture demonstrates PCI (Payment Card Industry) level encryption techniques by establishing SECURE ZONE.
  - The Secure Zone holds the data encrypted.
  - Demonstrates that even if the system were breached and data exfiltrated it cannot be decrypted outside of the defined Secure Zone.
- Direct Connect capability.
  - Provides an IPsec-encrypted private connection that also reduces network costs and increases bandwidth throughput.



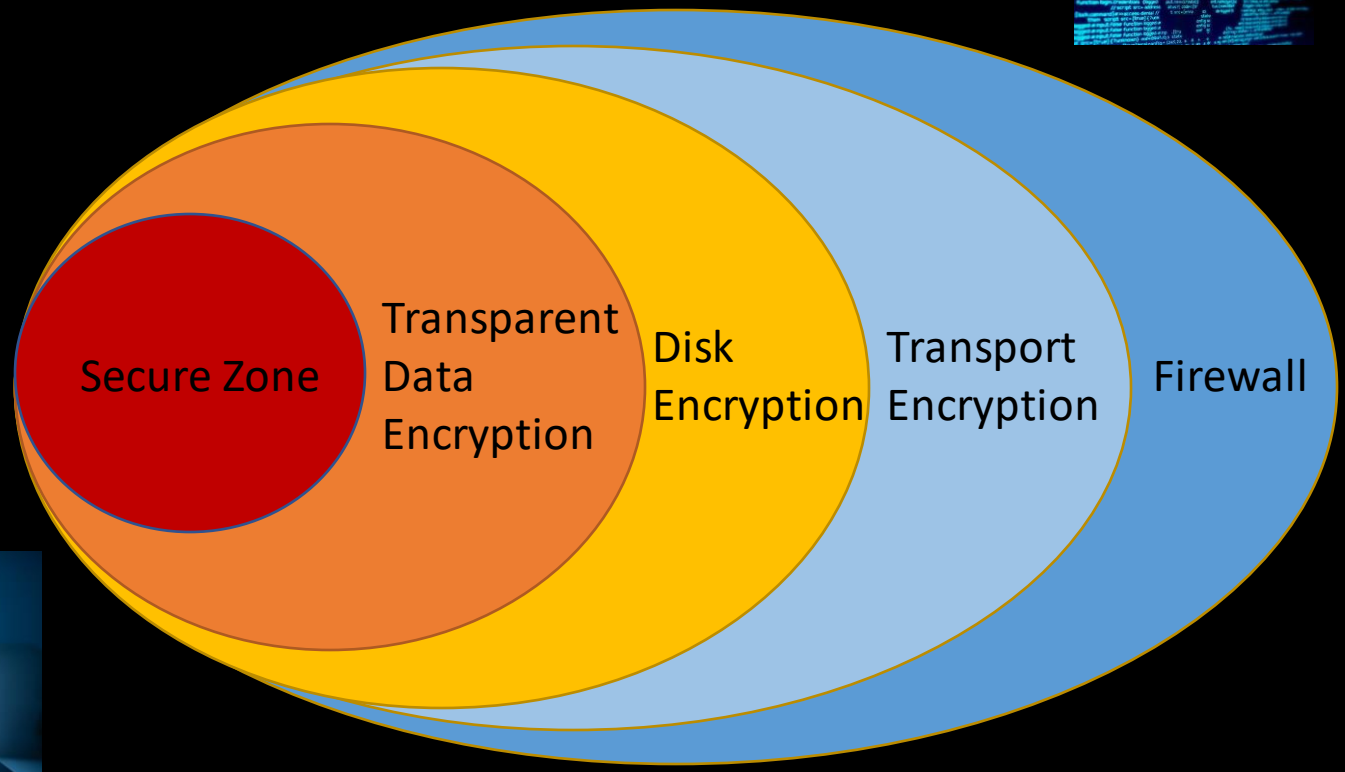
AMIP Security

- AMIP meets demanding DoD security standards.
  - Application is fully STIGed for Level I, II, and III (pending Army review)
  - Ready for Army assessment for ATO
- Multiple methods of authentication.
  - Secured authentication (CAC for Army, MFA/FIDO for others) (FIDO, Fast Identity Online)
- Role-based authorization enforced throughout the site.
- The System utilizes encryption for all connections.
  - Encryption of sensitive data inside Secure Zone
  - TLS 1.3 used between all components
  - Disk encryption used on all servers
  - TDE (Transport Data Encryption) used for SQL Server
- Hardware encryption used for additional protection of sensitive data.
  - Protects sensitive data in case of a data breach
  - Utilizes tokens to obfuscate key identification data
  - Tokenized data becomes unreadable if exfiltrated.
  - Remaining data is useless without a reference point

AMIP Security (Layered Defense)

As is best practice in the industry, AMIP utilizes a layered defense strategy to thwart bad actors intent on gaining access to the system, or intercepting data. This defense consists of five discrete layers, each designed to complicate any attempt at a data breach.

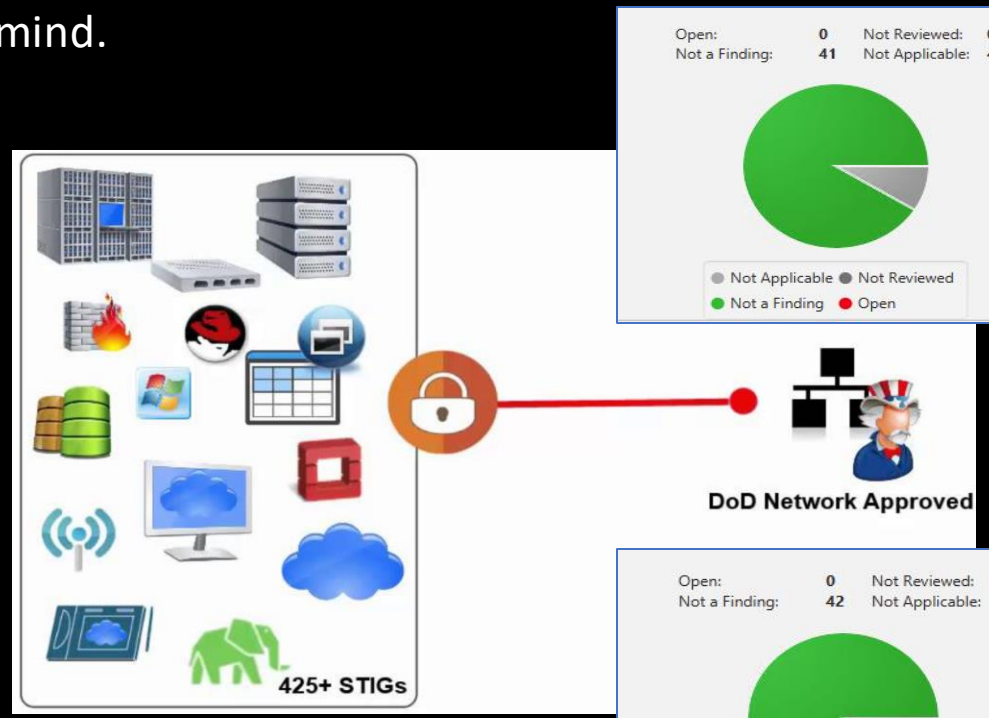
- Firewall
  - All communication is logged and routed through firewalls
- Transport encryption
  - TLS 1.3 is used for all communication between humans and machines and between machines and machines
- Disk encryption is used on all servers
- Transparent Data Encryption
  - Used for SQL Server data
- Strongkey tokenization
  - Used for sensitive data values



AMIP Security (DoD Configuration Standards Met)

All DoD production applications require an ATO (Authorization to Operate). To obtain an ATO, the applications must comply with technical testing and hardening frameworks known by the acronym STIG (Security Technical Implementation Guide). AMIP was designed and developed with STIG compliance in mind.

- AMIP is STIG compliant:
  - All Level I, II, and III STIGs have been met
  - NCDMM can provide the STIG Check file to any appropriate authority as of 3/1/2021
- AMIP supports multiple methods of authentication: CAC/PIIV for DoD-users and MFA for non-DoD-users.
- AMIP also has deployed a FIDO (Fast Identity Online) server, using StronKey hardware, that can be utilized by all users for MFA.
  - FIDO is the next generation of Multi-Factor Authentication
    - If CAC card is 8/10 on a security scale FIDO is roughly 8.5/10
- AMIP uses role-based authorization throughout the application.
- AMIP utilizes strong encryption throughout:
  - Encryption of sensitive data (See Strongkey below)
  - TLS 1.3 used between all components, restricted to high level cryptographic handshake between browser and application
  - Disk encryption used on all servers
  - TDE (Transparent Data Encryption) used for SQL Server



Advanced Manufacturing Intelligence Platform - AMIP (Flexibility)

- The AMIP Web Interface Architecture was designed to be portable and can be deployed to:
  - Any cloud service like AWS, Azure, Google, or IBM Cloud
  - On-premise in a single or multiple server architecture with or without internet connectivity
  - In a hybrid model where some resources are on-prem and some are in the cloud

- AMIP currently resides in Microsoft's Government Commercial Cloud – Azure GCC
  - GCC provides DFARS flow downs (CMMC L3), FedRamp High, CJIS, IRS 1075, DISA SRG L2 controls compliance
  - The deployment architecture is determined by the defined use case of the system and completely configurable by the system and database administrators

- AMIP runs in any modern browser with TLS 1.3 Encryption
  - Edge, Chrome, Firefox, Safari
  - Pages are optimized for swift load times

	Commercial	M365 "GCC"	M365 "GCC High"	M365 "DoD"
Customer Eligibility	Any customer	Federal, SLG, Tribes, DIB	Federal, DIB	DoD only
Datacenter Locations	US & OCONUS	CONUS Only	CONUS Only	CONUS Only
FedRAMP *	High	High	High	High
DFARS 252.204-7012	No	Yes	Yes	Yes
FCI + CMMC L1-2	Yes	Yes	Yes	Yes
CUI / CDI + CMMC L3-5	No	Yes^	Yes	Yes
ITAR / EAR	No	No	Yes	Yes
DoD CC SRG Level **	N/A	IL2	IL4	IL5
NIST SP 800-53 / 171 ***	Yes	Yes	Yes	Yes
CJIS Agreement	No	State	Federal	No
NERC / FERC	No	Yes^	Yes	Yes
Customer Support	Worldwide / Commercial Personnel		US-Based / Restricted Personnel	
Directory / Network	Azure Commercial		Azure Government	

* Equivalency, Supports accreditation at noted impact level

** Equivalency, PA issued for DoD only

*** Organizational Defined Values (ODV's) will vary

^ CUI Specified (e.g. ITAR, Nuclear, etc.) not suitable REQS US Sovereignty

aws | On-premise | Microsoft Azure

ncdmm.org

Conclusion

Additive Manufacturing technology is a force multiplier for the supply chain.

AMNOW enhances this multiplier by simplifying and accelerating the procurement process for Additive Manufacturing.

The AMIP system allows the Army to build upon Additive Manufacturing's advantages by streamlining the procurement process, encouraging innovation, tracking build data, and analyzing data to determine best practices/processes for a given application.

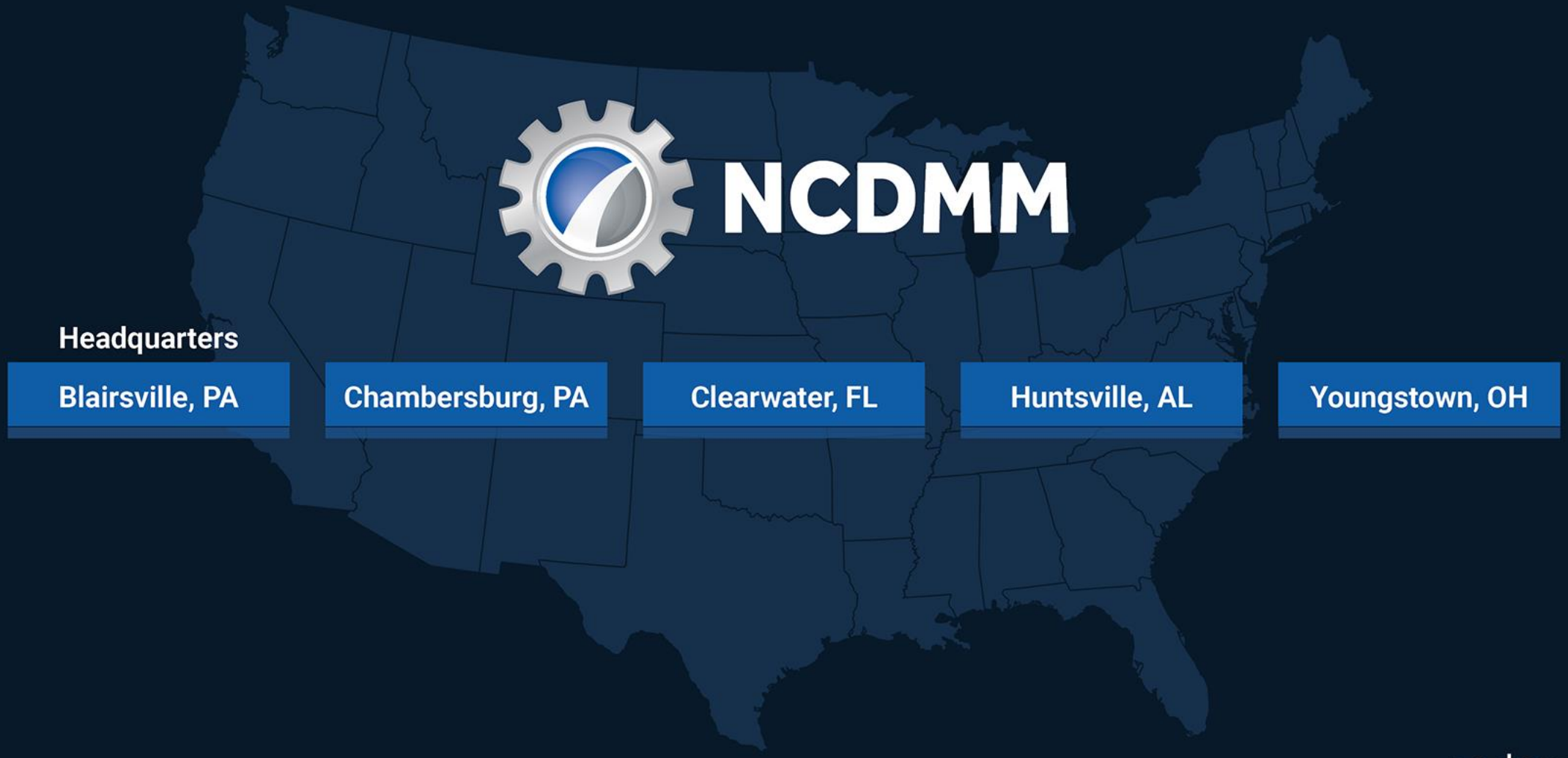
AMNOW/AMIP stands ready to support Army personnel.

NCDMM

Questions

LOCATIONS

NCDMM



ncdmm.org