

Disclaimer: Any opinions stated today are purely of my own and not necessarily those of DFAS, DISA or the DoD.

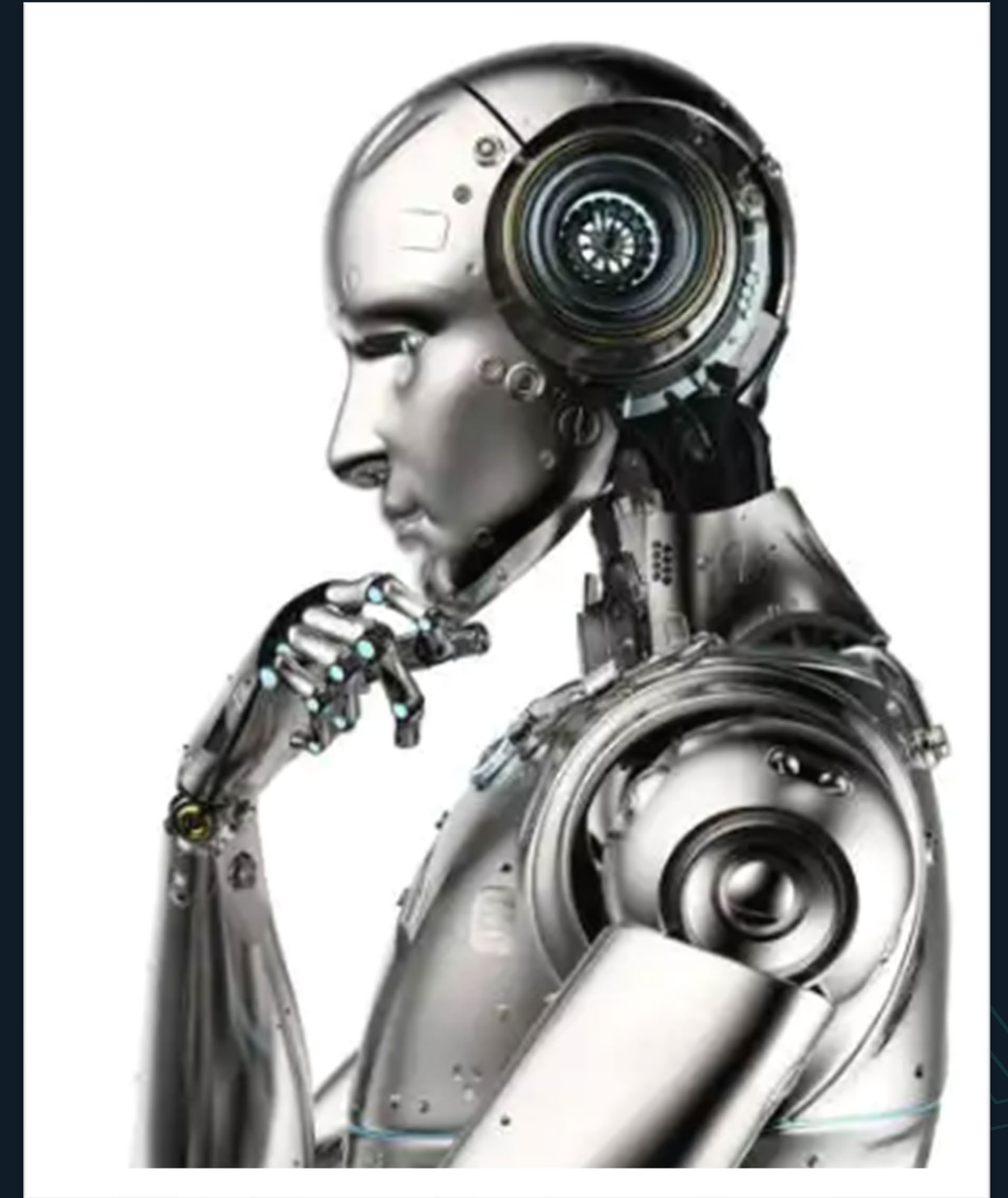


Beyond AI: Where Do We Go From Here?

Mr. Don Means
DFAS, Chief Information Officer
September 24, 2024

Agenda

- DFAS I&T Strategy Placemat
- DFAS I&T Strategy Measures
- ICAM – Impact to FY28 Audit Goals
- The Zero Trust Journey
- DRAS Modernization
- Artificial Intelligence (AI)
 - Video
 - Veracity of Data
 - Cybersecurity: AI Arms Race
 - ALERT
 - AI: A Double-Edged Sword



DFAS Information and Technology Strategy (FY25-29)

ENHANCING THE DFAS CUSTOMER AND EMPLOYEE EXPERIENCE THROUGH MODERN IT



Drive Innovation

Discover, develop, and employ disruptive IT that proactively and fundamentally impacts DFAS services

-  Robotic Process Automation
-  Cloud Maturity
-  Mobile Development
-  Expand AI
-  Digital Advancement

Focus on Our People

Retain and recruit a talented workforce to maximize opportunities and overcome challenges

-  Upskilling & Reskilling
-  Recruitment & Retention
-  Knowledge Management/Transfer






Accelerate Modernization

Identify and overcome environmental challenges, position DFAS to be tomorrow-ready, and flexible to evolve as mission requirements grow

-  DRAS-M
-  Reduce Legacy Systems
-  Modernize and Standardize Technology
-  DevSecOps

Strengthen Cyber Operations

Enhance cyber operations and security as we innovate and modernize the way we deliver capabilities and protect DFAS customers

-  ZeroTrust
-  ICAM IDP
-  ICAM AAP
-  Continuous Authorization (C-ATO)
-  Data Center Closure



ENHANCED CUSTOMER & EMPLOYEE EXPERIENCE

Fast, intuitive, and accessible applications and digital workplace

Empowered workforce able to achieve goals and deliver results

Automated and optimized processes with quality improvement

Secure and dynamic digital landscape

Superior business agility and improved efficiency

Ability to increase adoption pace with technological advancement

DFAS Information and Technology Strategy (FY25-29)

Objective Lead
Community

Best Practices Identification

Expand Intelligent Automation

Increase Bot Success Rates

Increase Labor Hours Through Deployment Automation

Reduce Cycle time needed for key Processes

Attract and sustain a premier workforce

Decrease average time to offer for Developer Roles

Increase DFAS I&T outreach at targeted universities

Increase DFAS' Federal Employee Viewpoint Survey

Implement Targeted Local Supplement for cyber positions

Adopt DevSecOps Methodology

Increase percentage of in scope DevSecOps systems

Increase percentage of developers within IT with expert proficiency on DevSecOps methodology

Decrease percentage of change failure rate

Mature cloud Readiness to Become Cloud First Organization

Increase Applications in Commercial Cloud

Increase Labor Hours Through Deployment Automation

Equip Employees with the Knowledge and Tools they need to deliver exceptional service

Increase competency for digital technology

Increase course utilization rate of DU courses taken

Establish and grow number of active Knowledge Groups

Establish a Data Management Strategy

Increase data assets cataloged in defined applications to track/monitor assets

Increase data domains assigned to data stewards

Reduce customer data request response time

Deploy Mobile Capabilities to Improve Customer Experience

Increase number of active users for mobile apps

Increase Customer Satisfaction Scores

Launch DRAS-M

Increase percentage of modules/systems completed

Increase timeliness through immediate transaction processing

Increase frequency of successful software releases using MVP

Accelerate Zero Trust Architecture and Framework Adoption

The number of zero trust target level activity gaps closed

Advance Digital Capabilities to Propel Innovation

Increase number of active users using low code platforms

Decrease average time to deliver end to end capabilities through digital platform

Reduce Legacy Systems

Perform App rationalization to aid system modernization

Decrease percentage of material weaknesses by retiring systems

Implement Enterprise Identity, Credential and Access

Percentage of IT Internal Control over Financial Reporting onboarded to authorized user authentication platform

Percentage of ICoFR systems onboarded to ICAM automated account provisioning

Develop Skills for Today and the Future of Work

Achieve compliance with 8140

Increase number of software developers proficient in COBOL programming language

Standardize Technology Platforms and Tools

Increase number of systems funded for modernization

Increase number of systems modernized to meet audit goals

Reduce percentage of systems unsupported by end of life hardware/software

Optimize Operational Resilience

Reduction in time to detect & respond to threats or vulnerabilities

Increase proactive incident detection rate of identity issues prior to user impact

Increase interactive response time of key applications from diverse points across the environment

ICAM – Impact to FY28 Audit Goals



Identity Provider (IDP)

- Centralized multifactor authentication for DoD CAC users and ICAM components
- Global Federated User Directory (GFUD)
- Leverages Microsoft Active Directory Federation Services (ADFS)
- Pilot MFA capability, Production solution planned for FY23



Automated Account Provisioning (AAP)

- ICAM user interface
- Self-service SAAR workflow
- Access Reviews
- Recertification
- Reporting
- Application Segregation of Duties (SOD)



Master User Record (MUR)

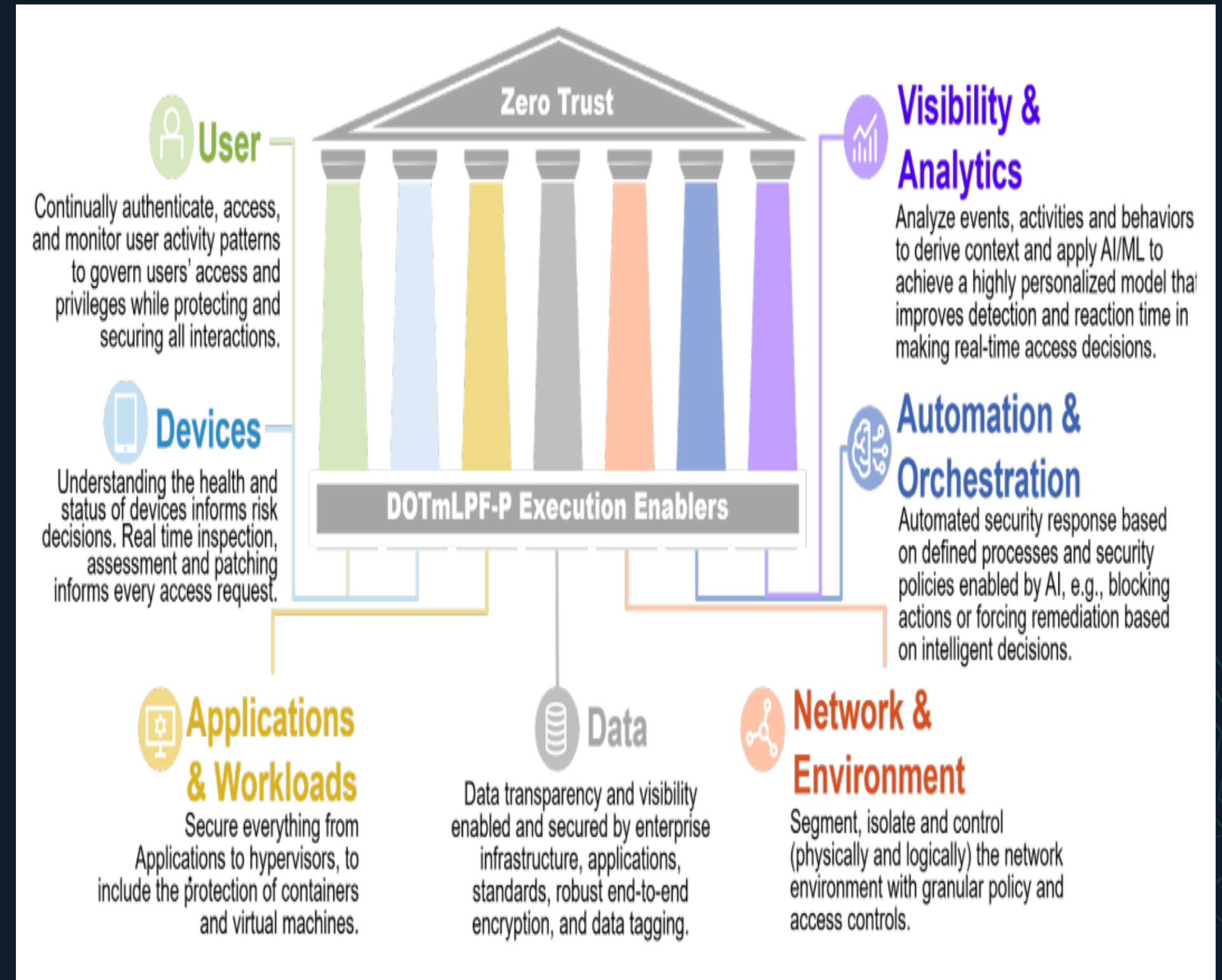
- DoD user data store
- Aggregation of authoritative data
- Enterprise Segregation of Duties
- API Service Account
- Provisioning Actions Status
- Programmatic updates



- IDP ensures only approved users have access to Financial Management systems
- AAP automates provisioning and de-provisioning, provides ability to perform required access reviews, and eliminates SOD conflicts at the application level
- MUR enables Federated Data from the entire Department of Defense to eliminate material weaknesses for Access Controls and Cross System SOD conflicts

The Zero Trust Journey

- ✓ **Multifactor/Continual Authentication**
- ✓ **Conditional Access**
- ✓ **DevSecOps**
- ✓ **Digital Rights Media / Data Labelling**
- ✓ **Micro-segmentation**
- ✓ **Security Orchestration and Automation**
- ✓ **User and Entity Behavior Analytics**
- ✓ **Cyber Threat Intelligence**





DRAS Modernization

DRAS PROBLEM

- Retired & Annuitant Pay Operations are limited by a complex system, requiring significant maintenance, offline support & batch processing that impedes services to customers
- Eight independent modules across four operating environments, using varying data structures with over 2.5 million lines of code
- System complexity hampers cyber security, timeliness and optimized processes
- DRAS is not positioned to support R&A Pay into the future

DRAS-M OBJECTIVE

- To deliver a reliable, cost effective, and flexible system that leverages advanced technology to support R&A pay well into the future

DRAS-M Project Outline	What do we get out of this?
<p>Phase 1 – Code Conversion</p> <ul style="list-style-type: none"> • Base Contract • Optional CLIN1 (Proof of Concept) • Optional CLIN2 (Code Conversion) 	<ul style="list-style-type: none"> • Succeed or Fail Fast (First Off Ramp) • Incremental Minimal Viable Product (MVP) of converted and refactored code, tested and delivered to cloud dev/test environment • Awarded to multiple vendors so we can down-select and choose best solution • Full baseline version of DRAS JAVA code ready to be modernized and deployed to production in Call Order 2
<p>Phase 2 – Incremental DRAS-M Modernization, Integration and Deployment</p>	<ul style="list-style-type: none"> • Incremental Minimal Viable Capability Release(s) (MVCRs) • Potentially awarded to multiple vendors to speed delivery • Includes architectural design and targeted enhancements
<p>Phase 3 – Customer Experience Enhancements</p>	<ul style="list-style-type: none"> • As DRAS-M modules are deployed, impacted customers get to take advantage of the enhancements • Full project delivery: 2029

Mission Impossible: Dead Reckoning

- [https://youtu.be/HF8BcUBUBb4?si= AueihYCWvFabQJd](https://youtu.be/HF8BcUBUBb4?si=AueihYCWvFabQJd)



Veracity of Data

Importance of accuracy and reliability of data in cybersecurity

Challenges in ensuring data integrity in the digital age

Veracity of Data Challenges

Data Inconsistency

Data Errors

Data Quality and relevance

Data security & privacy concerns

Data Volume and Velocity

Lack of data governance

Cybersecurity: AI Arms Race



AI as a tool for both attack and defense in cybersecurity



Dual nature of AI: enhancing security and developing sophisticated cyberattacks



Real-world examples include:
AI driven malware
AI based defense systems



Where do we go from here? Back to paper? Hyper-digital?



ALEERT

Advanced Learning and Evaluation for Risk and Transaction Monitoring

- ▶ ALERT is a highly sophisticated Artificial Intelligence application that can detect and flag transactions as potentially fraudulent prior to payment

- ▶ ALERT uses multiple AI Strategies to make predictions
 - ✓ Decision Tree supervised ML is used to classify or categorize transactions as either legitimate or potentially fraudulent using labeled data

 - ✓ Neural Networks are also used for deep learning through a hidden layer of connected artificial neurons to make predictions of fraud based on 60 different variables

 - ✓ Application can analyze a million transactions in a matter of seconds

- ▶ ALERT will continue to improve as new features are being added on inputs for predictions and more data is received



How does it work



**User Initiates
Change in MyPay**



**OPM Generates
Daily Change File**



**File uploaded to
DFAS Cloud**



**Valid transactions are
processed without
further review**



**Flagged transactions are
manually reviewed by a
human before processing**



A ALERT

Advanced Learning and Evaluation for Risk and Transaction Monitoring

FOCUS AREAS



4

3

2

1

Models

SUPERVISED/UNSUPERVISED

4

Supervised Models:

- Supervised models are trained using labeled data, where each data point is tagged as either fraudulent or legitimate.
- These models learn to identify patterns and characteristics within the labeled data to make predictions on new, unseen data.

3

Unsupervised Models:

- Unsupervised models are trained using unlabeled data, so the model learns patterns and structures without explicit fraud labels.
- These models identify anomalies or deviations from the norm within the data, which can indicate potential fraud.

2

1

Profiles BEHAVIORAL ANALYSIS

Behavioral analysis in AI and fraud detection involves the use of advanced analytics to identify and flag potential instances of fraud or unusual activities. This approach leverages machine learning and behavioral analytics models to understand evolving patterns in real-time. By monitoring user activity and transaction behavior, it can detect and prevent fraudulent activities and unusual behavior within an organization's operations.

4

3

2

Models

1

Data IMPROVEMENT

AI can improve data for fraud detection in several ways:

1. Enhanced Pattern Recognition
2. Predictive Analytics
3. Accelerate Decision-Making
4. Adaptive Learning

Overall, AI improves data for fraud detection by providing more accurate and timely identification of fraudulent activities, predictive capabilities, and adaptive learning to stay ahead of emerging fraud trends.

4**3***Profiles* **2***Models* **1**

Continual ADAPTING

AI can adapt to changing online fraud by leveraging advanced machine learning algorithms and predictive analytics. One approach involves utilizing historical fraud data to train AI models, enabling them to recognize evolving patterns and behaviors associated with fraudulent activities. Additionally, AI can continuously learn from new instances of fraud and adjust its detection mechanisms in real time to adapt to emerging threats. This adaptive capability allows AI to stay ahead of evolving fraud tactics and enhance its effectiveness in mitigating online fraudulent activities. Furthermore, the incorporation of anomaly detection and behavior analysis enables AI to dynamically adjust its fraud detection strategies, thereby maintaining its relevancy in the ever-changing landscape of online fraud. (Stay informed with investigations)

4

Data

3

Profiles

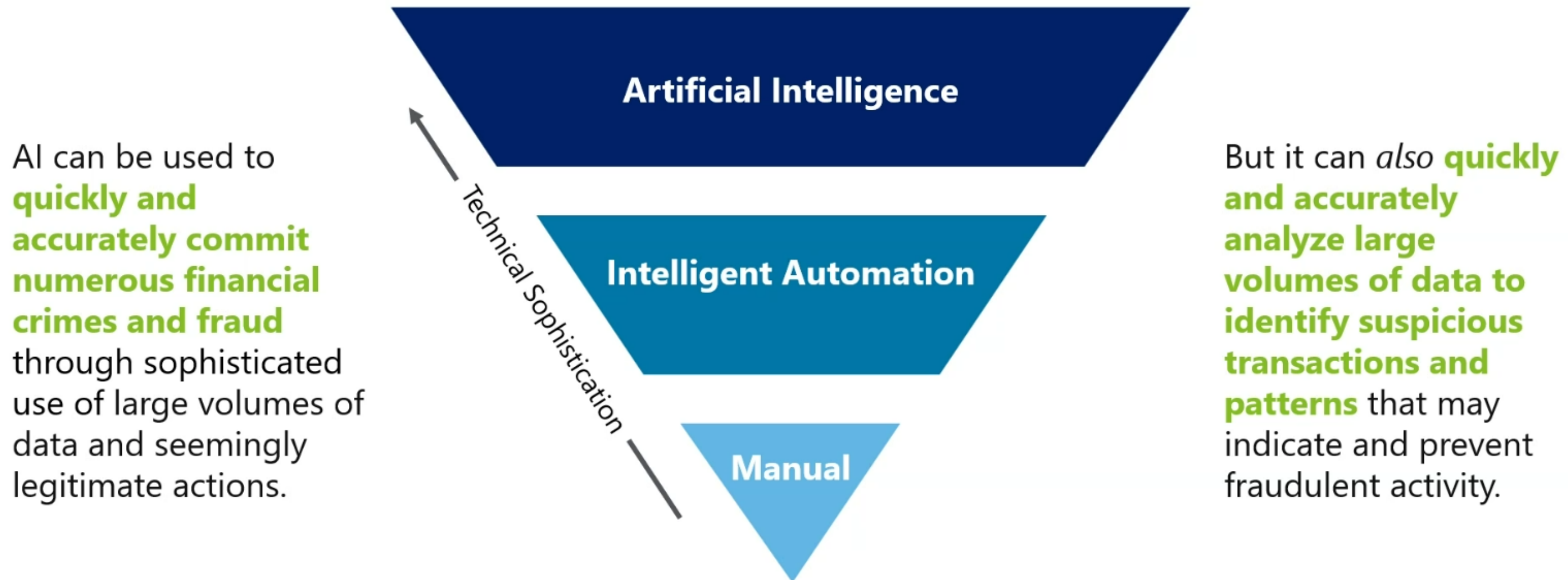
2

Models

1

Artificial Intelligence: A Double-Edged Sword

AI increases the sophistication of both attack *and* response efforts.



Questions?



Disclaimer: Any opinions stated today are purely of my own and not necessarily those of DFAS, DISA or the DoD.

Backup Slides



Visual or Audio Data

- Unique security challenges posed by visual and audio data
- Vulnerabilities
 - Interception
 - Alteration
 - Manipulation
- Security measures
 - AI-based anomaly detection systems
 - Paper? Hyper-digitalization?



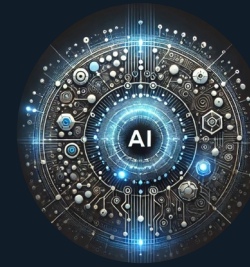
Generative AI

Technology that can generate new content, such as images, text, music or even videos to mimic similar content created by humans

End Points – What does it look like for DoD?



Text generation to create human like text



Data Augmentation generating synthetic data to augment existing datasets for training machine learning models



Image generation to create images based on parameters and styles



Simulation and prediction to create realistic simulations for training purposes in fields such as robotics



Video Synthesis to create new videos or automations based on input data or styles



Creative applications which will help generate ideas or designs



Mr. Don Means, Jr. CIO

Don Means Jr. is a Class of 1989 Illinois Institute of Technology graduate. He used his Bachelor of Science in Engineering as the foundation for a stellar career in IT, with 34 years of service, including as an officer in the U.S. Navy and as a civilian in the United States government. He has a Masters Degree in National Resource Strategy from National Defense University and is a Harvard Senior Executive Fellow.

Mr. Means currently serves as a senior executive at the Defense Finance and Accounting Service as the agency's Chief Information Officer and Director of Information Technology. In this role, he oversees the I&T responsible for enabling the Department of Defense to uphold its fiscal responsibilities for all financial transactions, including payroll and accounting services, enterprise systems for financial transactions, and infrastructure support. Moreover, he ensures that all networks and transactions made through those networks are secure and cyber defended.

Prior to recently joining the Defense Finance and Accounting Service, Mr. Means served as a senior executive and director of the Defense Information Systems Agency's Operations and Infrastructure Center. Mr. Means oversaw the Defense Information Systems Agency's largest component, with a global workforce of 6,100 or one-third of the agency's military, civilian, and contractor personnel. As center director, he led a multi-billion dollar cybersecurity portfolio and, in support of the Department of Defense's mission, he was responsible for maintaining and defending the world's third largest IT network next to the United States and China: the Defense Information Systems Network. His center installed and maintained enough optical fiber to wrap around the world more than two times and defended the Department of Defense's global network from hundreds of millions of attacks daily. Without his team's expertise and the capabilities they deliver, the United States cannot fight or support an ally in war. He has dedicated his professional career to serving the United States and is among few who have the experience of doing so as a member of the armed forces, a civilian and as a member of industry, having spent several years as a senior engineer and analyst with Raytheon.

His commitment to the mission and to driving solutions has been recognized with numerous awards including the Defense Meritorious Service Medal, Black Engineer of the Year Award, and most recently, the Exceptional Civilian Service Award. Mr. Means regularly engages with colleges and universities in support of their efforts to develop the future cyber workforce. To that end, he is currently serving on the Illinois Institute of Technology's College of Computing Board of Advisors.

