

Embracing Change:

Transformation



Innovation

Frank Konieczny

AF Chief Technology Officer

Office of Information Dominance & Chief Information Officer

March 2016

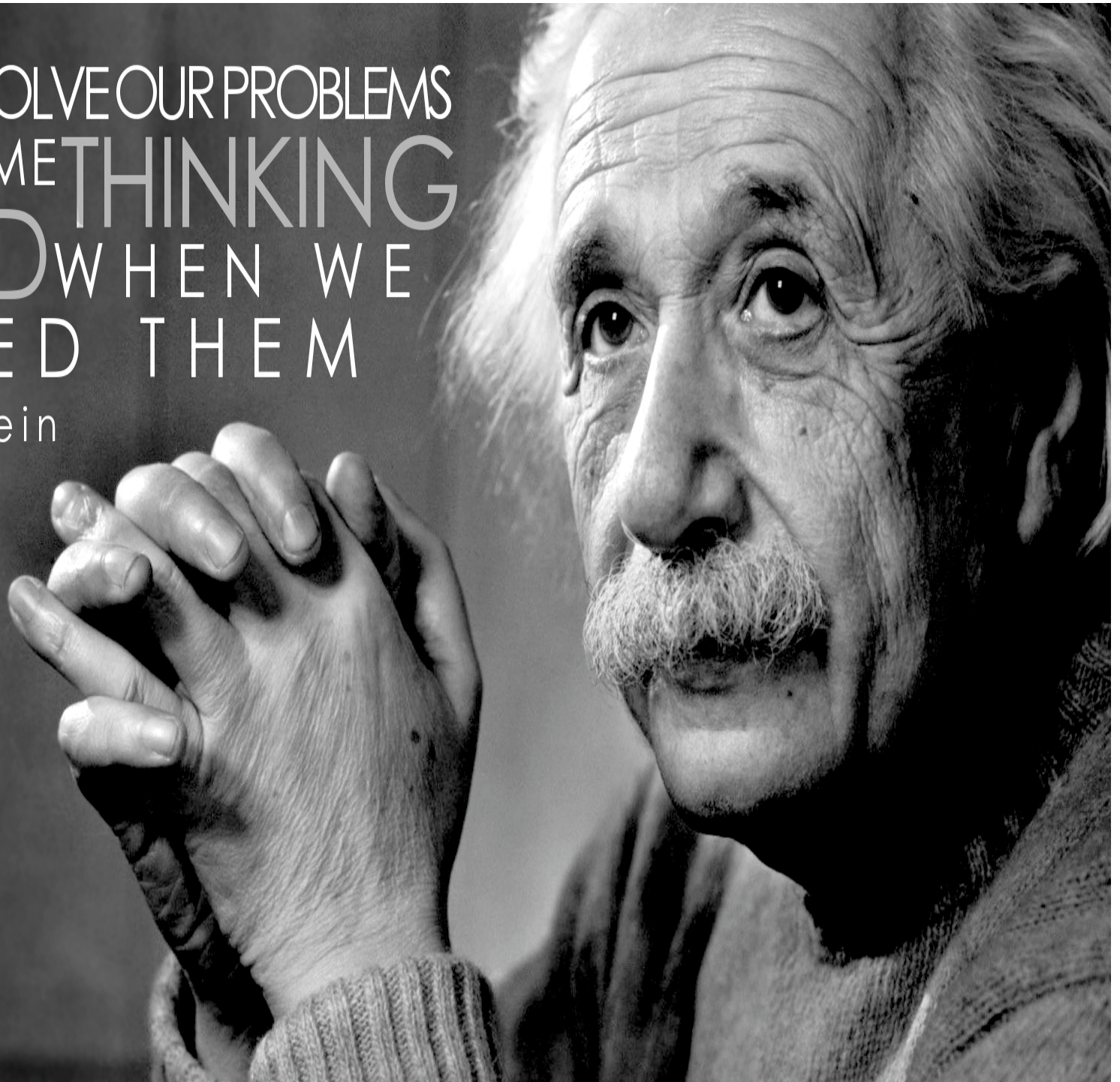


U.S. AIR FORCE



WE CANNOT SOLVE OUR PROBLEMS
WITH THE SAME THINKING
WE USED WHEN WE
CREATED THEM

- Albert Einstein





U.S. AIR FORCE

Outcomes Based Approach

- Focus change on meeting critical objectives/goals
- Customer Involvement
 - In control
 - Understood
 - Keeps informed
- Provider Activities
 - Specific objectives
 - Accomplishment metrics for progress
 - De-prioritizing of other activities
- For SAF/CIO, the Information Dominance Flight Plan – Goals:
 - Provide Airmen Trusted Information
 - Organize, Train, Equip & Educate Cyber-Airmen to be experts in cyberspace
 - Deliver Freedom of Action In and Through Cyberspace
 - Optimize the PPB&E of Cyberspace Investments



U.S. AIR FORCE

Embracing Change through Innovation Governance

- AF Information Technology Governance Executive Board
 - 3 Star decision board on enterprise information technology
- AF Data Panel
 - Supports Data Usage across the AF
 - Determination/registration of authoritative data sources
- Mobile Enterprise Service Panel
 - Supports mobile services across the AF
 - Includes network, device management, device selection/control, application management/control, Internet of Things, Platform IT
- AF Cyber Innovation Forum
 - Coordination of cyber innovations capabilities across the AF
 - Includes design thinking, education, initiative selection and assessment



U.S. AIR FORCE

Utilize Commercial Innovations

- Defense Innovation Unit-experimental (DIUx)
 - Connection with innovative, venture capital-based companies
 - Supports problem discussions/analysis with related commercial companies
- In-Q-Tel
 - Wide portfolio of technology advanced companies – invests in these
 - Space operations, mobility, data analytics, cyber defense, bio research, electronics
- Allied Minds
 - Converts FFRDC projects into commercial products
- Assess commercial products through PlugTest
 - Evaluate commercial add-ons/connections to current systems
 - Use Other Transaction Authority to contract for pilot efforts



U.S. AIR FORCE

“As a Service” Innovation

- Driving Issues
 - Shortage of airmen – need to be mission focused
 - Training/re-training requirements due to rotation
 - Maintaining up to date equipment and services
- Several services can be considered commodities that can be bought/received as required; operated by skilled technicians
 - Electricity
 - Phone
 -



U.S. AIR FORCE

Network as a Service

- Provide network as a service for entire base (coverage includes flight lines, etc.)
 - Landline (NIPR/SIPR)
 - LTE: Private (NIPR) and Public
 - WIFI (SIPR/NIPR) where LTE signal is inadequate
 - VOIP plus instruments
 - LMR Connectivity Support
- Provide periodic updates of network equipment to keep up with current releases
 - Outage window will be outside of normal business hours unless network outage is not disruptive
- Manage all network equipment
 - Standard maintenance/patching of equipment (SLA)
 - Standard replacement of faulty equipment (SLA); option for emergency replacement
 - “Help Desk” support for receiving and resolving network related issues
- Status COP
 - Provide network status information to commander dashboard
 - Inform CNDSP of perceived incidents
- Provide as a monthly charge (based on usage)



U.S. AIR FORCE

IPN as a Service

- Provide base data center services
 - Provide and manage virtualized environment
 - Manage special hardware “hoteling” -- legacy
 - VDI capability
 - Storage- file shares
 - Standard services (e.g., AD, DNS)
 - JIE security suite
 - Monitor/manage utilities (e.g., electricity, HVAC); support green initiatives
- Interface with Mission-CND provider regarding application incidents
- Provide services within GFE building or via vendor supplied pods
- Provide on a monthly charge based on usage

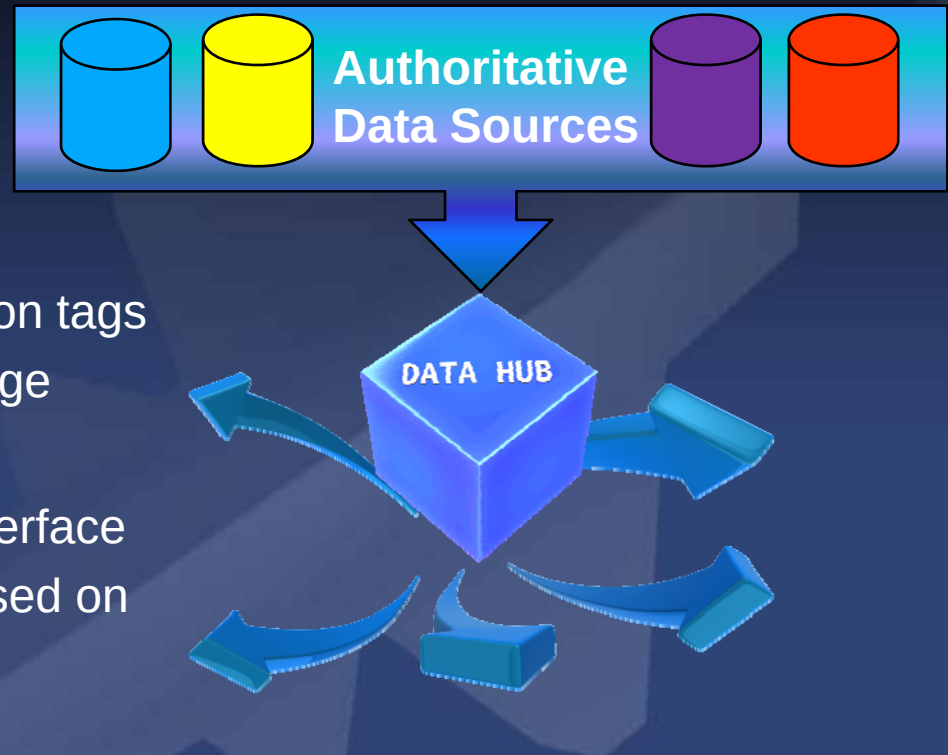




U.S. AIR FORCE

Data Hub (Data as a Service)

- AF Data Management
 - Authoritative data
 - Provenance score
 - Access, security and disposition tags
 - Register ADS for AF/DoD usage
- Data Hub
 - Search to support analysis/interface
 - Auto extraction/translation based on
 - User requests
 - Application requestsinto “information assets”
 - Tagging of the information asset for control
 - Preferred web service access to information assets
- Currently piloting several tool sets

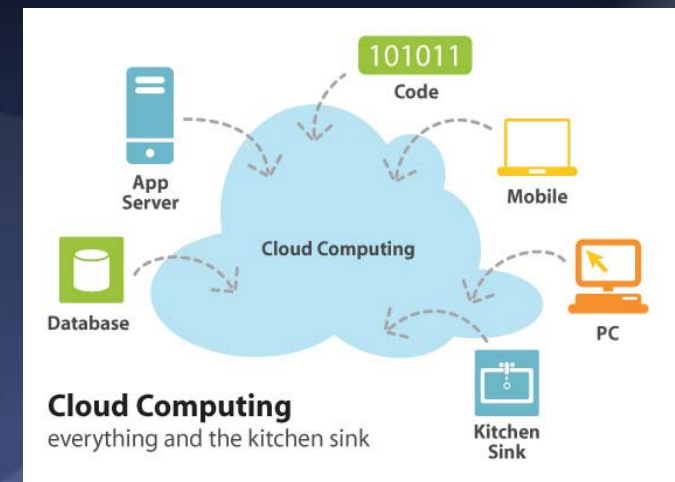




U.S. AIR FORCE

Computing/Storage as a Service

- Joint Information Environment Drivers
 - FDCCI and Core Data Center Consolidation (DOD CIO Directive to move all appropriate apps to core data centers by FY18)
 - Mission and cost efficiencies -- consolidation of base owners/tenants applications into one base data centers or core data centers
- Approx 5000+ AF applications
 - Identify base/MAJCOM unique applications and “Duplicative” applications across bases
 - Automated tool support to identify and categorize applications
 - Established Managed Service Office (C3N&I) to manage transition/migration
- Focus on efficiencies that cloud computing can provide
 - IaaS
 - PaaS
 - Storage as a Service
 - Software as a Service
- Applicable to CDCs, IPNs, and Commercial Cloud Providers





U.S. AIR FORCE

Computing/Storage as a Service

- Commercial cloud capability assessments
 - Based on data that will be stored/processed
 - Controls are specified in the Cloud Computing Security Requirements Guide – FedRAMP certification is the base (level 2 public releasable data) on which additional controls are levied
 - Several commercial cloud vendors are under evaluation for data impact levels 4 and 5
- Piloting Software as a Service
 - Personnel application
 - Email
 - Specific applications
- Issues
 - Acquisition Strategy including direct contract relationships
 - Funding strategy when moving to a commodity based model



U.S. AIR FORCE

Innovation thru AF Target Baseline

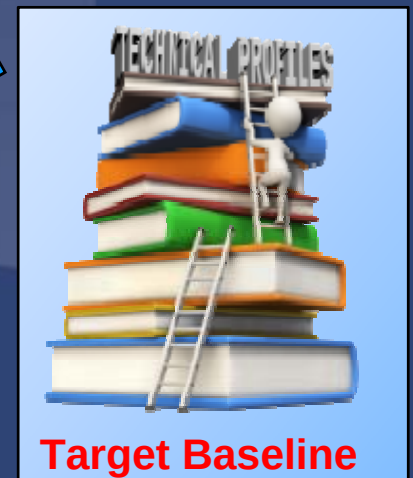
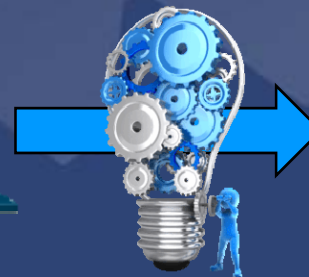
- Specifies the standards, protocols, guidelines and implementation constraints/requirements for the future state of the AF information technology – *the “To-Be” infrastructure*
- Releases based on user community expressed needs
 - Specify what capabilities/outcomes are desired
 - Frame these in terms of use cases/scenarios/questions
- Develop Technical Profiles (specifications) to describe technical solutions that resolve the use case issues; use EA identified IT functions as base for technical profiles
- Working on Release 4 TPs
- Basis for Implementation Baseline (C3N&I)



Functional Issues



Use Case Based
Scenarios



Target Baseline

Target Baseline (TB) is future state – drives capability evolution



U.S. AIR FORCE



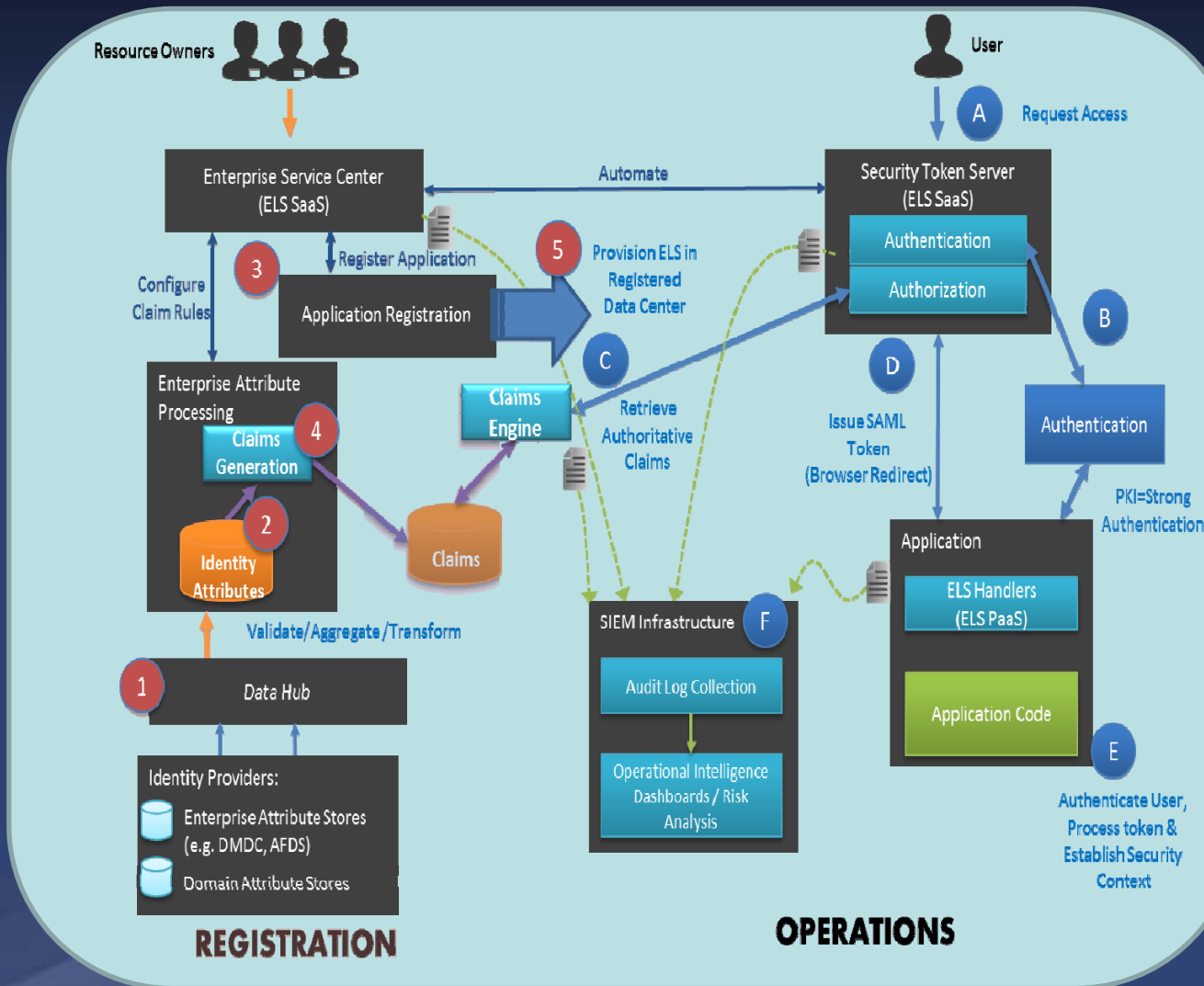
- **Enterprise Level Security**
- **Virtual Application Data Center**
- **Enterprise Mobility**
- **Analytics**
- **Mission Thread Analysis**
- **Commander Operational Dash Board**



U.S. AIR FORCE

Enterprise Level Security

JIE Access Control Pilot



Benefits

- ❑ Warfighters are able to focus on the mission with faster access to needed information systems
- ❑ Decrease the number of administrators / access is dynamically managed by change attributes
- ❑ Scalable role management through self-service
- ❑ Lower C&A Cost - Standardized application security implementation
- ❑ Trusted identities (single version of the truth)
- ❑ Common Enterprise Standard Approach
- ❑ Standards based & "cloud- friendly" protocols

Claims Management

- ❑ Requires quality attributes sources
- ❑ Requires Resource owner to determine claims/roles in terms of user attributes for access control



U.S. AIR FORCE

ELS Innovation

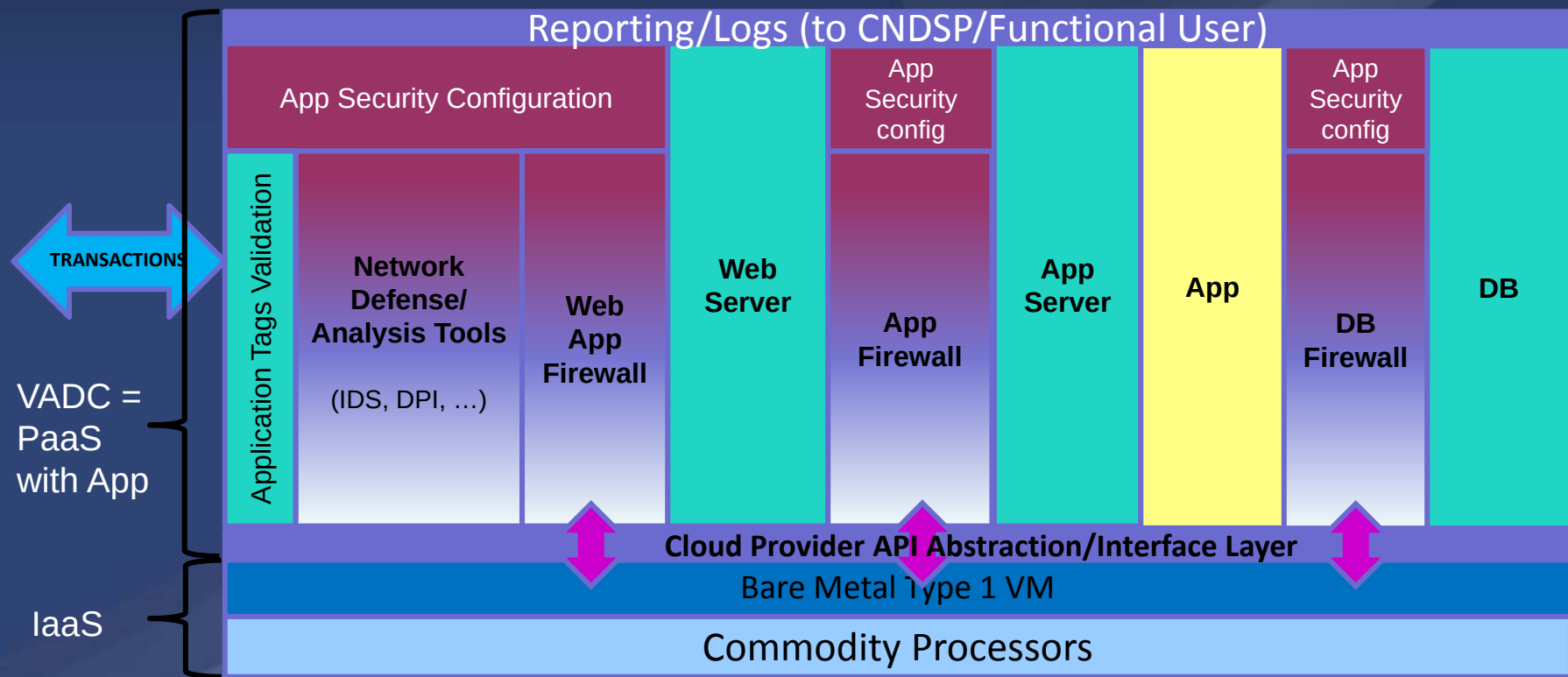
- Evolution of capabilities through 8 agile spiral developments
- Current state: production milCloud instance being installed
- Extension to IPN, Commercial Cloud and SIPR milCloud
- Research into determination of type of authentication and geo-location/time of access request to restrict degree of access
 - Mobile device access via other than CAC
 - First responders and related type access
- Extension of ELS to unstructured document access
 - Collaboration Sites
 - File Shares
 - Email
 - External to DoD Domain for authorized access



U.S. AIR FORCE

Virtual Application Data Center

- All components virtualized and containerized to a specific application in its own VDC
- Current trend for security tool is to support a virtual capability – also, accommodates Software Defined Networking (SDN)
- Security Policies are configured to the criticality of the application





U.S. AIR FORCE

AF Enterprise Mobility

- Five lines of effort determining enterprise requirements and way forward
 - Base Network Infrastructure (NaaS Pilot)
 - Device Lifecycle Management
 - Mobile Device Management (for all devices including some mission legacy)
 - Device selection (based on mission), acquisition and disposal including BYOAD
 - Mobile Capabilities Management
 - Application development/standards
 - Application registration and release/approval
 - Mobile Mission Integration
 - Other than phone devices required for mission
 - IOT: sensors, drones, trucks, cameras, smart homes, roads...
 - Platform Wireless Capability
 - Weapon system integration/requirement
- Cross cutting policy/legal effort
- Piloting efforts are being planned for each line of effort





U.S. AIR FORCE

Analytics

- Using big data to solve problems and identify issues
- Predictive Analysis
 - Fuel
 - Maintenance
 - Time-based collaboration
- Threat Analysis
 - Network anomalies thru machine learning
 - Predictive analysis
 - Insider Threat Detection
- Classification Analysis
 - Document tagging for access and disposition
 - Personnel next-role forecasting based on actual/projected skills
 - ...

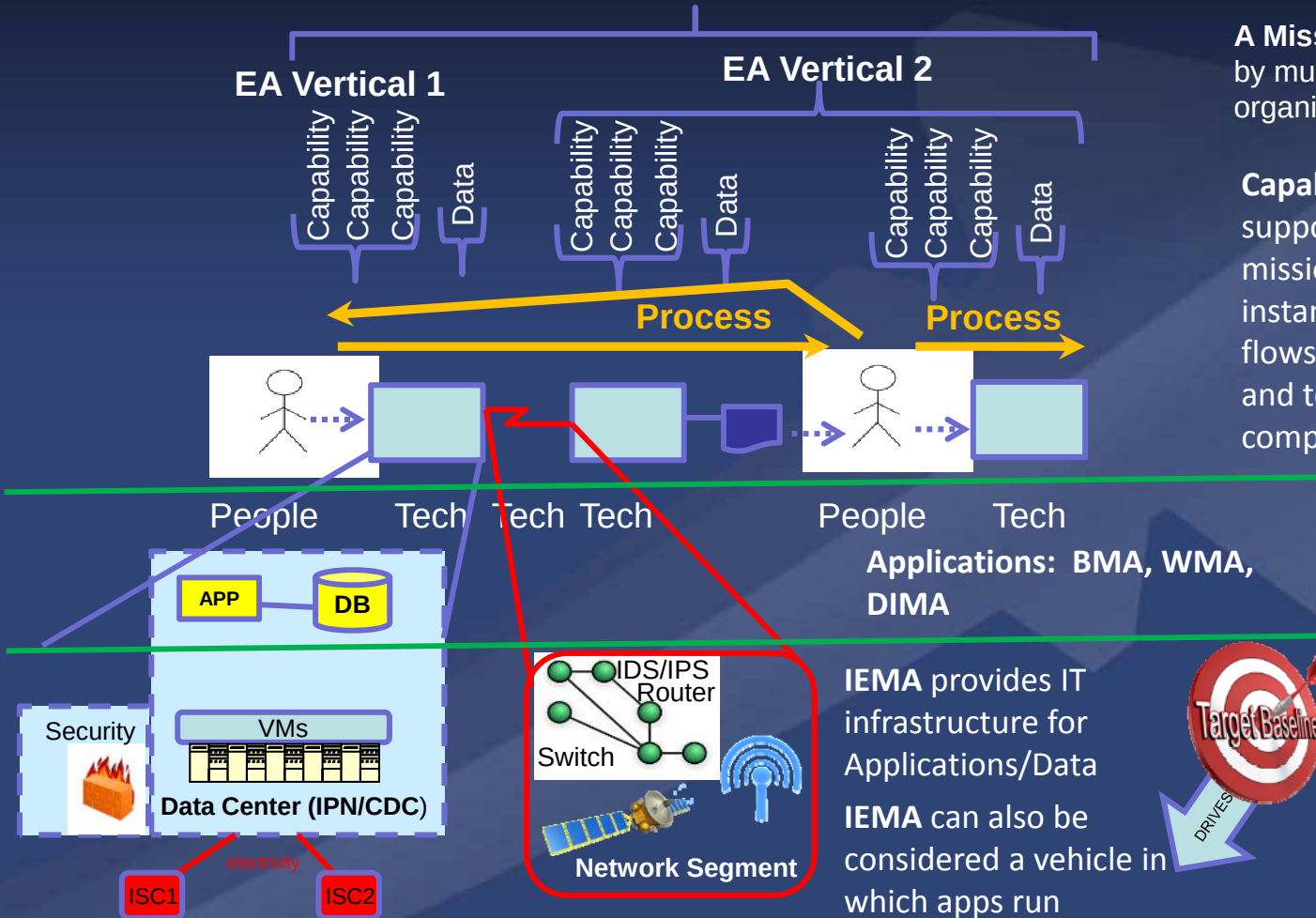




U.S. AIR FORCE

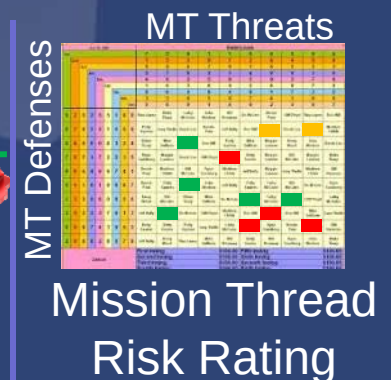
Mission Thread Identification and Risk Management

Mission Thread



A **Mission Thread** is supported by multiple capabilities/data organized in EA verticals

Capabilities/Data supporting a specific mission thread are instantiated in process flows, personnel actions, and technology components.



IEMA provides IT infrastructure for Applications/Data
IEMA can also be considered a vehicle in which apps run



U.S. AIR FORCE

Commander Operational Dash Board



Base Level View

Mission Thread → Weighted Risk Score: **xx/100**



Network

- Bandwidth
- Availability
- Alternative Configuration Switch



Threat

- Old Known
- New Identified
- Insider
- Honey Pot/Block



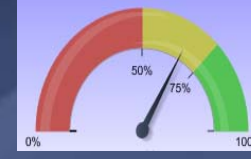
Defense

- Updates Status
- Patch Status
- Alternative Configuration Switch



Vehicle

- Maintenance
- Support Status
- Alternative Vehicle



Personnel

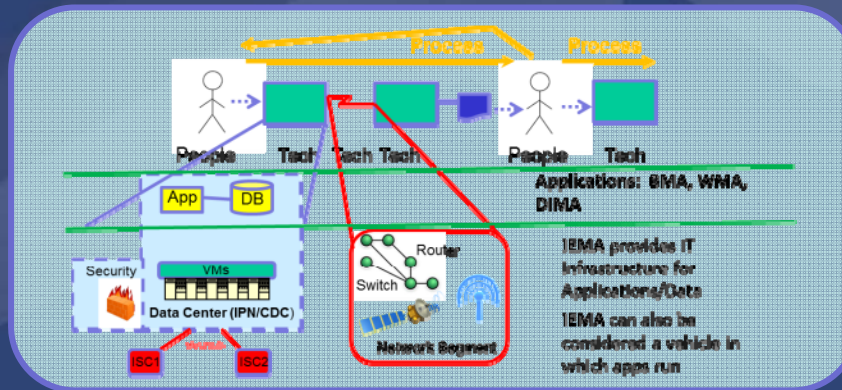
- Readiness
- Training Status



Manual Ops

- CM
- Process Checks

Potential Threats





U.S. AIR FORCE

DoD Transformation/Innovation: Joint Information Environment

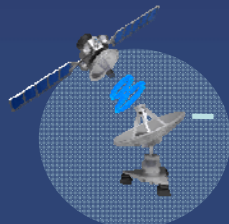
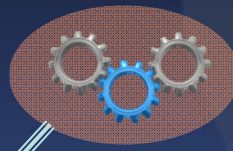
Internet Access Point



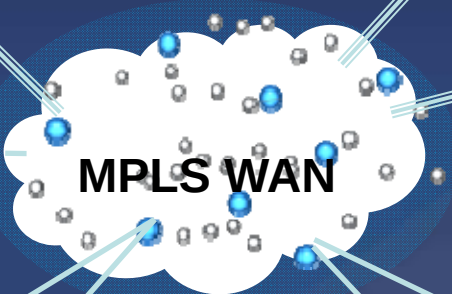
Partner Gateway



Enterprise Ops Center



SATCOM



Core Data Center

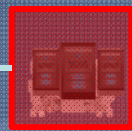
- "cloud" capabilities
- Optical Core connectivity
- Tier 3 data center



Base



Installation
Processing Node
-- Essential
mission apps



Special Purpose
Processing Node
-- Contained
capabilities

Base



Installation
Service Node
-- Enterprise
Services
-- No applications



Data Center Consolidation

- All applications are to move to Core Data Centers (CDC) by FY18 unless mission/cost justification is provided
- Base data centers are consolidated into Installation Processing Nodes (IPN)
 - Mission-critical applications that must operate in a DIL environment
 - All tenants utilizes the IPN on base
 - Cyber Security Stack for outside base communications
- Special Purpose Processing Nodes (SPPN)
 - Special processing that has no external personnel (i.e., outside of the SPPN facilities) accessing the systems (e.g., hospital)
 - Connectivity to DODIN through the IPN/CDC security stack



U.S. AIR FORCE

Questions

