Adaptive IT Innovation

Frank Konieczny

AF Chief Technology Officer

Office of Information Dominance & Chief Information Officer

March 2015

U.S. AIR FORCE

On the Road to Innovation

- **How can the AF effectively integrate new IT technologies into a mission?**
- **What processes could be used?**
- **Are there tools/patterns to support this?**
- **How does this intersect with Joint Information Environment (JIE) planning?**

Where to Start?

- **Distill current description of the activities that the AF is responsible to accomplish from AF Enterprise Architecture (2010)**

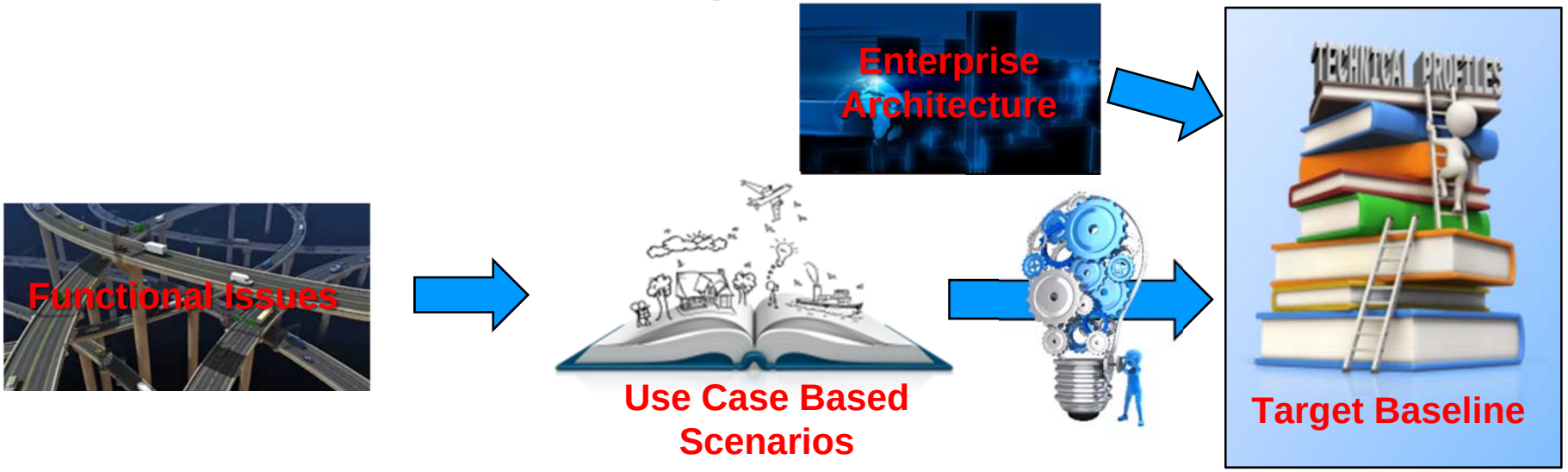
- **Determine which Mission Area best represent the Information Environment: IEMA**

- **Categorize IT functions supporting the AF mission:**
  - **Presentation – 5**
  - **Enterprise Management – 16**
  - **Enterprise Applications – 3**
  - **Application Foundation – 10**
  - **Data/Information – 13**
  - **Computing Services – 9**
  - **Storage – 8**
  - **Network/communications – 19**
  - **Device Ops/Mgmt – 3**
  - **Network Ops/Mgmt – 15**
  - **Application Ops/Mgmt – 6**
  - **Security – 23**

Total: 130

How to Approach the Problem?

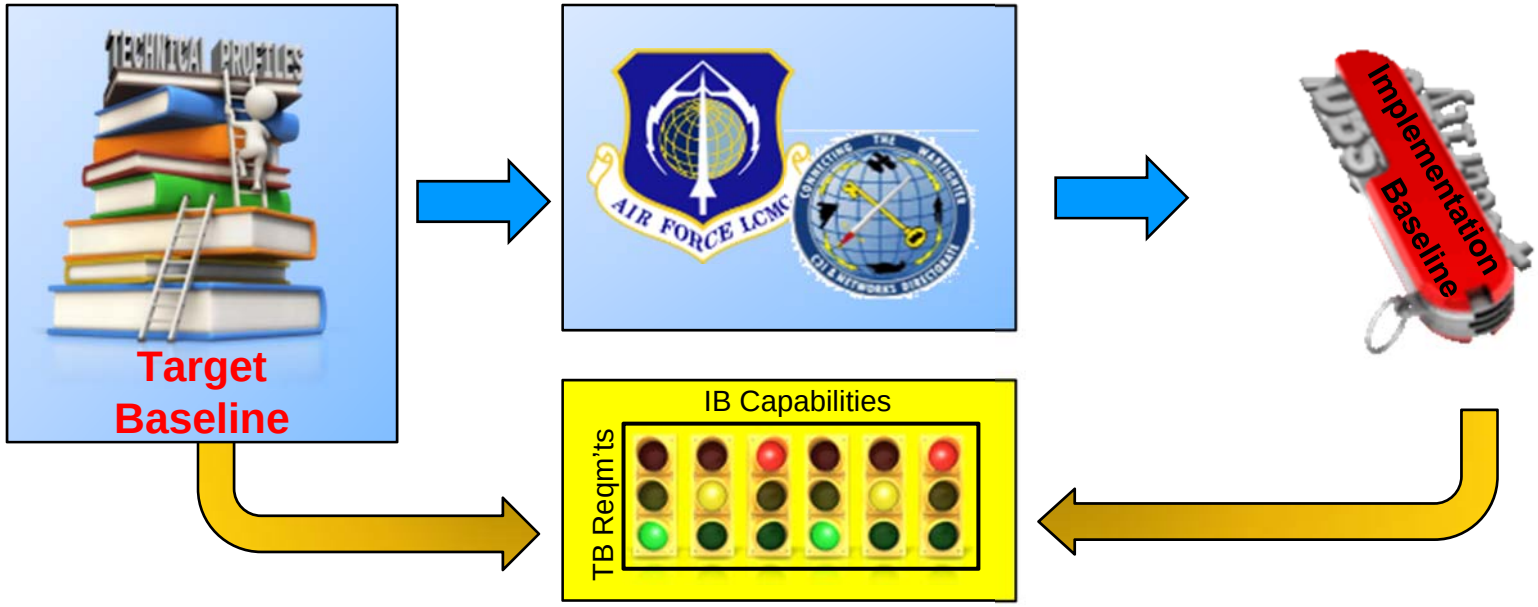
- Ask the user community
  - Specify what capabilities/outcomes are desired
  - Frame these in terms of use cases/scenarios/questions
- Develop Technical Profiles (specifications) to describe technical solutions that resolve the use case issues; use EA identified IT functions as base for technical profiles



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

How do Real Products get Delivered?

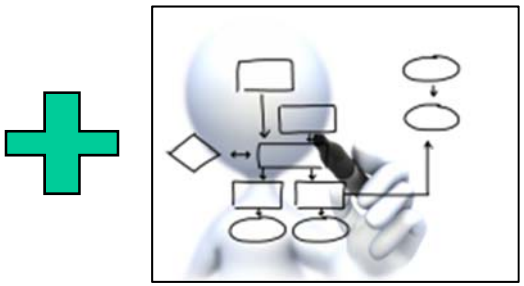
- The IT Function Technical Profiles together describe capabilities/products that can be acquired/developed/delivered
- AFLCMC delivers these capabilities as the **Implementation Baseline (IB),** and IT capabilities in the Common Computing Environment services catalog
- Since TB is future state, all TB requirements may not be yet deliverable; plan to attain complete requirements



TB-IB Completion Chart

What do I do with these IB Capabilities?

- Implementation Baseline (IB) provides standardized components/architecture for application usage
  - IB definition is about speed
  - Speed through a more rapidly provisioned accredited environment
  - A consistent environment/patterns for mission capability developers
- New and modernizing applications are required to use these standard components
- If additional capabilities are needed, must be Target Baseline compatible or needs to be added through the Target Baseline process



Application Code

- Fielded capabilities are part of the Operational Baseline (OB) – this includes specific infrastructure and application configurations

What is all this?

- A ***governance process*** **to systematically inject new enterprise level information technologies and infrastructure**
- A ***set of standards, protocols, requirements and service components to support*** **building current and future state of the IT enterprise**
- **Description of the current and future state of the IT enterprise environment**
- **Three baselines which are approved by established AF-wide Configuration Control Boards (CCBs)**
- **Collectively called the AF Consolidated Enterprise IT (CEIT) Baselines**

Baselines Reviewed

- **Target Baseline (TB) - specifies the standards, protocols, guidelines and implementation constraints for the future state of the AF IT infrastructure – the *"To-Be" infrastructure***

- **Implementation Baseline (IB) - the set(s) of acquisition selected products and their configurations that implement the Target Baseline – for new and modernized applications, the *instantiation* of the target (TB) into an operational application infrastructure**

- **Operational Baseline (OB) - the set of components of the IB configured and deployed across the AF IT infrastructure to provide the required warfighter capabilities and performance – the *"As-Is" infrastructure***

CEIT Strategy

- **Separate mission capability from infrastructure**
- **Migrate, Build, Use capability on provided IT infrastructure**
- **Use services to deliver capability in modular, incremental approach**
- **Get out of the business of hosting mission and business systems or applications**
- **Procure hosting services from a provider (e.g., DISA, vendors, etc.)**
- **Establish and manage infrastructure as a system**
  - Based on managed services and commoditized IT
  - Provide standard infrastructure platforms/patterns
  - Adopt standards-based approach
- **Adopt effective processes/approaches/patterns**
  - Recognized and supported governance
  - Develop, test & integrate new capability in the operational environment
- **Drive these innovations into the Joint Information Environment initiative**
  - IDT Support
  - Operable capabilities

Timelines

- **Target Baseline**
  - Each major number release has two segment releases: Scenarios and Technical Profiles
  - Goal is 45 working days for the each segment release to the TB CCB
  - Three to four releases during the year
- **Implementation Baseline**
  - Tempo of IB releases to keep pace with technologies, greater commoditization, and ultimately more commonality and lower total life-cycle costs
  - There needs to be a level of stability for acquisition and development to be viable similar to commercial development
  - IB 3.0 development focuses on business systems use cases and limited C2 mission systems
  - Mid cycle “dot” releases, e.g., 3.1 Enterprise Services and Managed Platforms, support adjustments and additions prior to next major annual release
- **Operational Baseline**
  - As items are fielded

User On Ramp: Target Baseline

- **Target Baseline Scenario Workshop**
  - Off-site discussions held to determine the topics/use cases of interest from the AF community for the forthcoming releases
  - Open to all AF personnel
  - Selection of final topics collectively made based on estimated workload to be accomplished within the 45 working day window
  - Scenarios/Use Cases not included in the forthcoming release tabled until the next workshop
  - Agility/adaptability maintained by focusing on current issues

- **Out-of-cycle capability review**
  - When there is a mismatch between a desired tool and TB capability, we determine if the TB needs to be updated to incorporate the new features
  - Updates will be incorporated in the next TB release

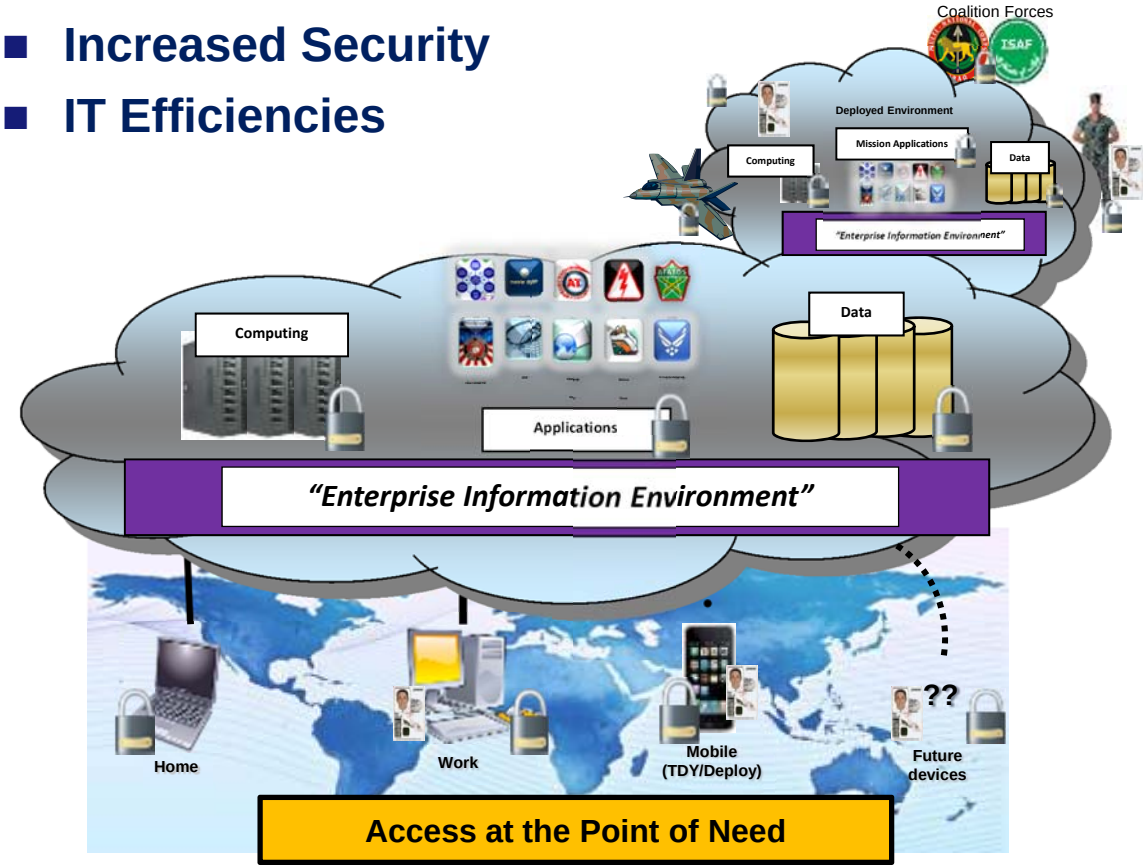
User On Ramp: Implementation Baseline

- **SAF/CIO A6 Mission Area Integrators (MAI)**
  - MAIs will coordinate with the C3N&I Managed Service Office (MSO) to migrate/modernize your application using the latest IB components.
  - MSO takes MAIs and Acquisition Process requirements as the point for providing capability to user/customers
  - Coordination includes establishing the provisioning of the development, test and production environments.

- **IB Technical Working Group Meeting**
  - All Functional Areas invited to participate in IB definition.
  - TB & OB members participate to incorporate consistency, traceability, and executability.
  - Supports identifying and filling gaps.

DoD Transformation/Innovation: Joint Information Environment

- Mission Effectiveness
- Increased Security
- IT Efficiencies

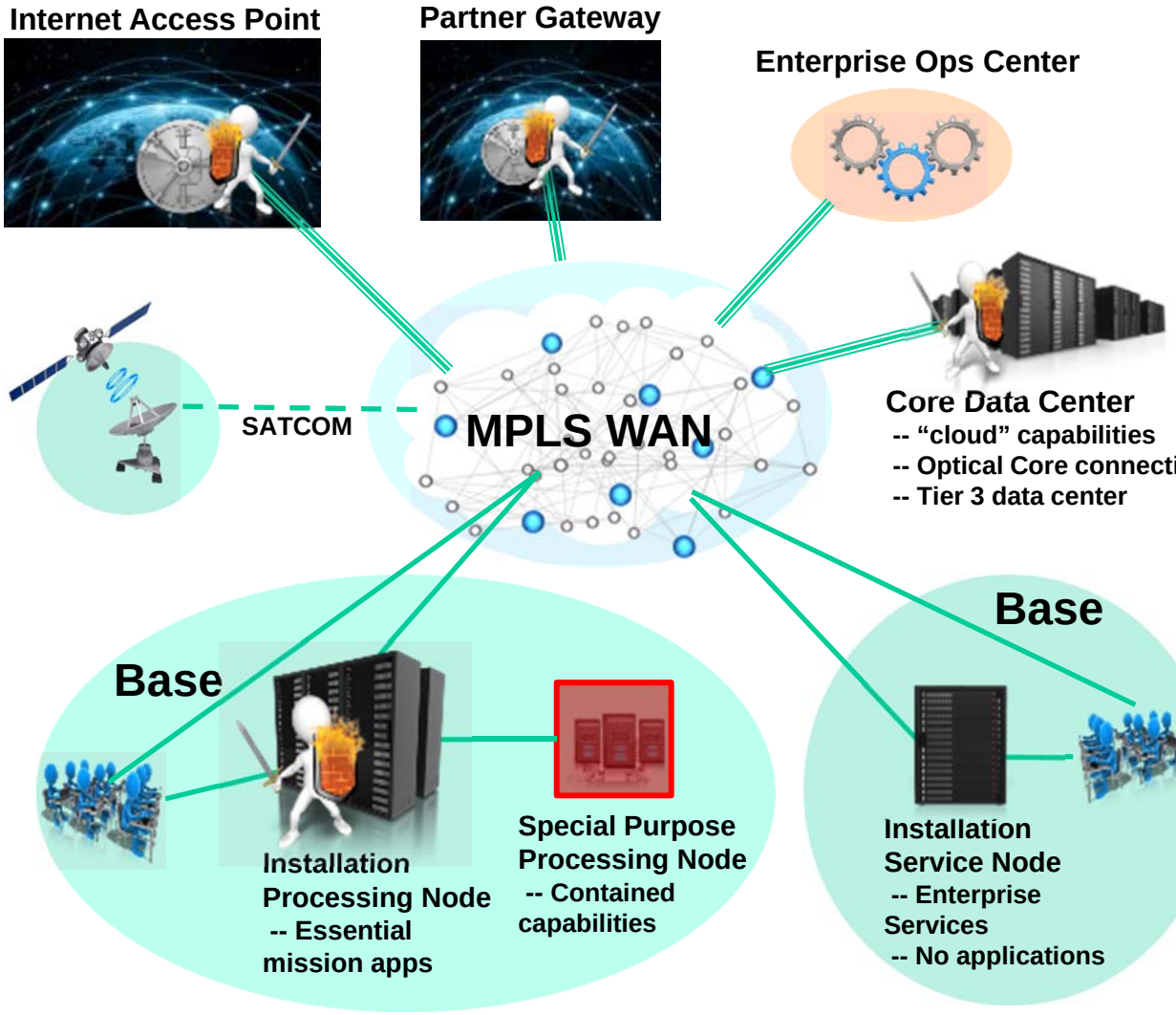


Big Rock Focus Areas

- Network Normalization
- Data Center Consolidation
- Single (Cyber) Security Architecture
- Identity and Access Management
- Enterprise Services

TANK directed development of JIE Way Ahead (16 Dec 11)

DoD Transformation/Innovation: Joint Information Environment



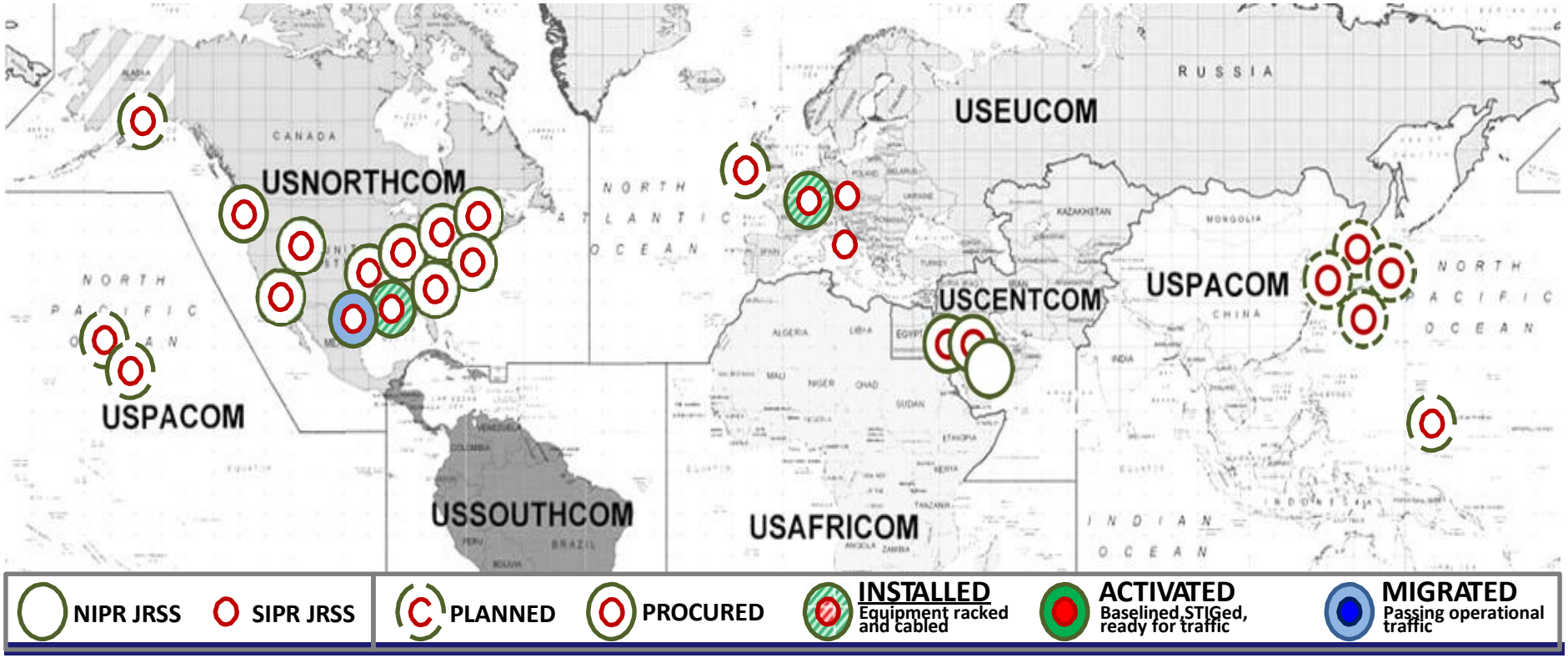
Data Center Consolidation

- 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

DoD Transformation/Innovation: Joint Information Environment

Network Normalization – Joint Regional Security Stacks (JRSS)

- Replaces AF Gateway and Base-to-Base network construct
- Encompasses NIPR/SIPR, SATCOM, Mission Partner Networks,...
- Integrates cyber security capabilities



INNOVATION

Results

Results – Target Baseline Release 1

Summary Use Cases:

1. **How to expedite user access to enterprise applications/network resources?**
   More effective and consistent way to maintain and update application and data access controls that would lessen system administrator handling
2. **What should we use for migrating to a cloud environment?**
   Standardization of components to establish a virtualized data center and software components that would represent a standard Platform as a Service (PaaS) capability

TB Outcomes:

1. **Enterprise Level Security (ELS)** – Automated method to support application/data access authorizations based on a *person's attributes* acquired from authoritative sources, e.g., billet, security clearance, location, completed training
2. **PaaS components** – standard web/application/database component requirements that comprise a PaaS standard and associated virtualization requirements
3. **Virtualization Components** – virtualized environment management, hypervisors, communication, virtual storage

Results – Implementation Baseline Release 3

Common Computing Environment (CCE) Platforms

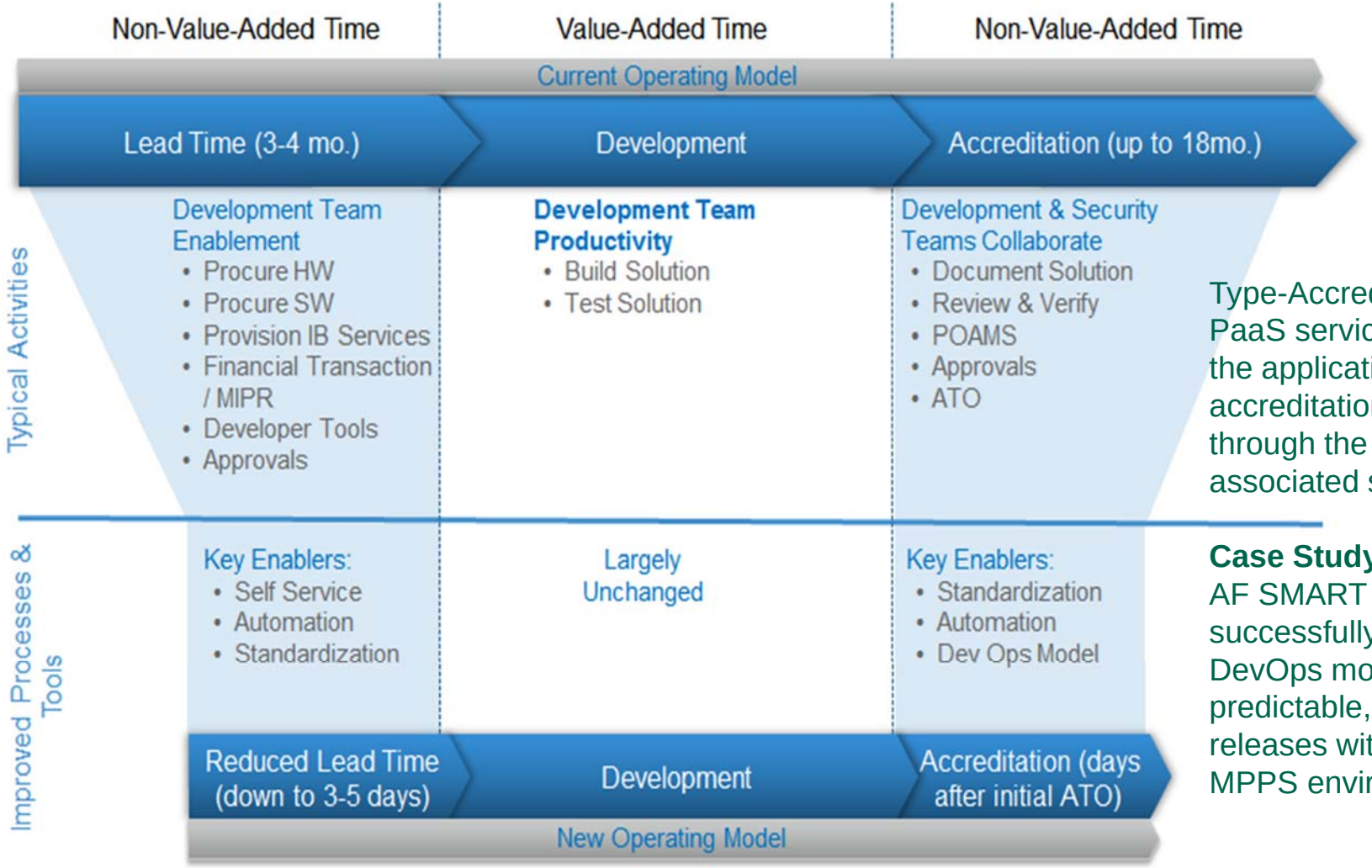
- **IB roadmap provides AF Mission Area Integrators with stable standards needed for application planning**
  - **Today: IB v3.0 w/ Focus on Platform Services; Implements TB Rel 1**
  - **Roadmap: IB v3.1 w/Focus on Enterprise Services (e.g. Messaging, Security, etc..)**
- **Platform standardization provides AF CCE with the ability to lower cost and improve security**
  - **Necessary for scalable operations & management**
  - **Necessary for automation and orchestration**

IB 3.0 Platforms

Microsoft	Java	Databases
• Windows Server 2012 R2 • Microsoft Internet Information Server (IIS) 8 • Microsoft .NET Framework 4.5 Optional: • SharePoint 2010 • SharePoint 2013	**Option 1** • Red Hat Enterprise Linux 6.x • JBoss Enterprise Web Server (EWS) • Red Hat JBoss Enterprise Application Platform (EAP) 6.2 **Option 2** • Red Hat Enterprise Linux 6.x • IBM WebSphere Application Server 7 • IBM HTTP Server Version 7.x (as bundled with WAS AS 7) **Option 3** • Red Hat Enterprise Linux 6.x • Oracle WebLogic Application Server 11gR1 • Oracle HTTP Server 11gR1	• Oracle 11g • Microsoft SQL Server 2012 • MySQL 5.5 • IBM DB2 Advanced Enterprise Server Edition • [NoSQL DB – Currently Evaluating Options] **Access Control** • Dynamic Attribute Based Access Control • Java/.NETt Handlers

Results: Implementation Baseline Release 3

Increasing Ratio of Value-Added Time to Non-Value-Added Time



Type-Accreditation of PaaS services accelerates the application accreditation process through the inheritance of associated security control

Case Study:
AF SMART application successfully moved to DevOps model with agile, predictable, application releases within DISA MPPS environment

Results:
TB Rel 1- IB Rel 3.0

Anticipated ROI:

- More secured applications: automated authorizations
- More expeditious access: Airmen productive upon arrival
- Consistent model for PaaS and CNDSP reporting: fewer Airmen needed for maintenance and management activities with increased level of situational awareness
- C&A inheritance from PaaS/ELS components

Status:

- ELS initial implementation under development in milCloud;
- Testing with real applications planned in Mar 2015; ATO in Apr 2015
- ELS meets JIE DoD IDAM Strategy and Reference Architectures
- ELS and standard PaaS defined in IB 3.0
- AFGM (Sep 2014) mandates the use of the TB 1.0 and IB 3.0 for all new and modernized systems

Results: Operational Baseline

- **Automated Asset Inventory**
  - **Persistent tool set to support inventory sustainment**
  - **Computing/Storage – Hardware/Virtual**
    - **USAFE Pilot**
    - **10 Base Pilot**
  - **Configurations – COTS tools/licenses**
- **Application Inventory**
  - **Overlay on asset inventory**
- **JIE/FDCCI Influences**
  - **Consolidation into JIE-specified data centers**
    - **DoD and Commercial Data Centers**
    - **AF Base Installation Processing Centers (for critical base mission apps)**

Results:
Target Baseline Release 2

Summary Use Cases:

1. **How can network traffic analysis be performed when services, e.g, ELS, requires end-to-end encryption between requester and provider?**
   - Package the application with its own network security services
   - Perform the network analysis as part of the application package
2. **How can applications in milCloud be moved to a commercial provider with minimal configuration change?**
   - Package application along with network security services, managed via configuration files, to facilitate migration between cloud providers

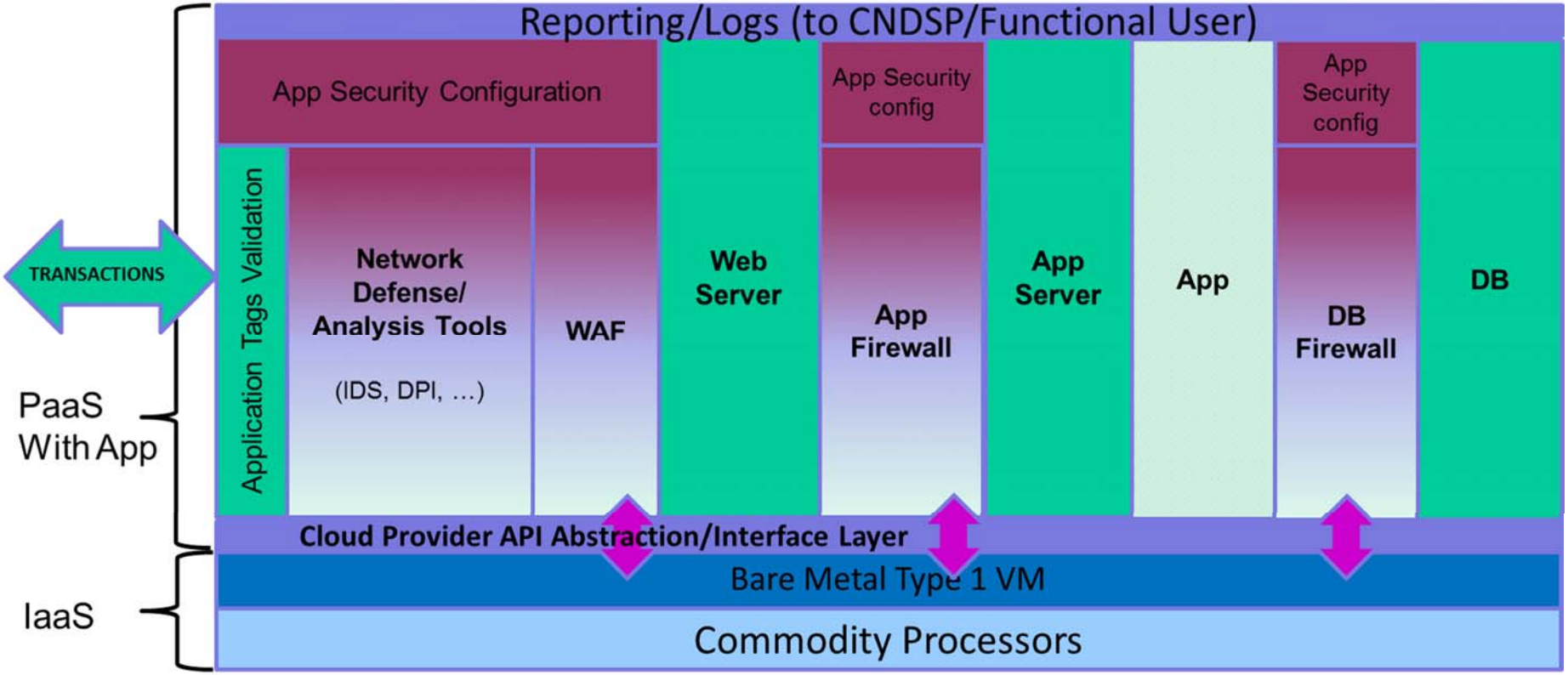
TB Outcome:

- **Virtual Application Data Center (VADC):** package standard PaaS construct with inherent virtualized network analysis (IDS/IPS), web application firewall and database firewall.

Note: each release revisits and improves upon existing Use Cases to accommodate innovation and new guidance

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



Results – TB Release 2

Anticipated ROI:

- Increased security (built-into the app package)
- Standardized CNDSP reporting requiring fewer airmen
- Whitelisted VADC firewall settings requiring less maintenance airmen
- Capability to move between data centers without app modification; just edit configuration files, requiring fewer Airmen to administer

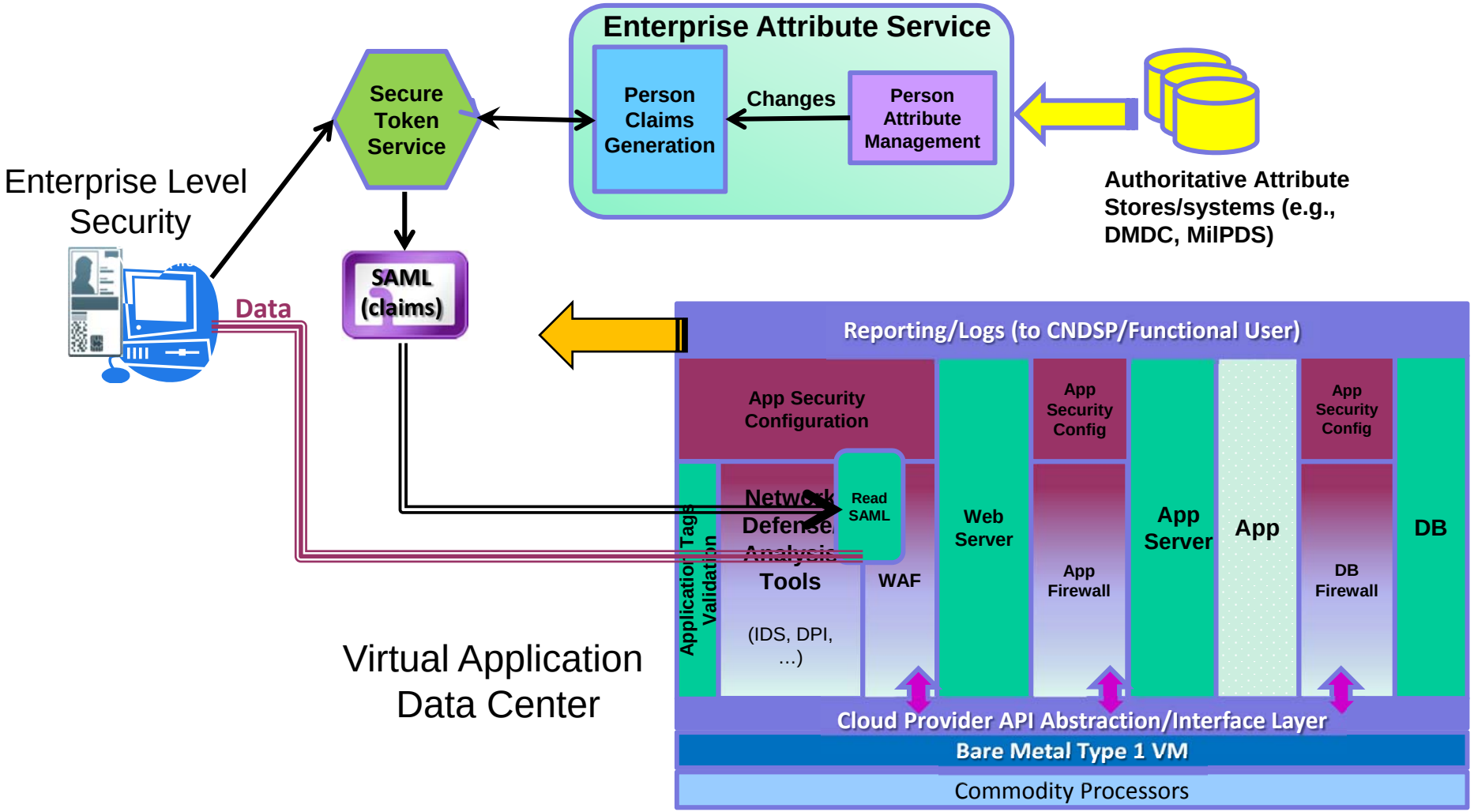
Status:

- CIO Memo (Feb 2015) mandates the use of the TB 2.0 and IB 3.0 for all new and modernized systems
- VADC concept being researched by AFRL; support from AFSPC/AFLCMC and DISA for test/evaluation
- Test pilot application (PAMS) early 2015

TB 1 & 2 Release Synergy

- **Security paradigm shift** to defending the mission information at the application layer:
  - Security-Encapsulated Application & Data Enclave (SEADE)
    - Enterprise Level Security (ELS) provides dynamic access control at the application/information layer
    - Virtual Application Data Center (VADC) concept tailors the defense to the application layer
- **Simplifies CND**
  - Configured as standard PaaS capabilities with minimal maintenance
  - ELS is a service that is used by applications
  - Anomaly reports are application tagged providing extensive information
  - Can configure to auto-reload if certain anomaly threshold reached
- **User response**
  - Effectively eliminates internal DoD domain latency due to network defense appliance saturations

Security-Encapsulated Application and Data Enclave (SEADE)



IB 3.1

- Incremental point release between major versions
- Incorporates shift from open PaaS to Managed Platforms
- Portability to host in DISA DECCs, milCloud, JIE Installation Processing Nodes data centers, other dedicated environments, and secure commercial cloud
- Incorporates enterprise services as provided by DISA, AF, other Services/Agencies, and commercial providers "as a Service"
- Provides more ready incorporation of services into a Utility VDC

TB Release 3

Summary Use Cases:

1. (Mobility) How do we manage mobile platforms on the enterprise?
   - Need secure connection to the network over WIFI/4G/LTE
   - Secure, standard, flexible connections across the aerial, space and terrestrial layers
   - Standardization of mobile comm capability and device registration across all bases
   - Use of soft certs for authentication
2. (Enterprise Info Management) How do we perform enterprise search for information?
   - Making data available enterprise-wide (data tagging)
   - Capability to find and manage information to support legal and other missions
   - Capability to restrict access based on information content & need to know
3. (Data Mgmt) How do we manage and integrate data from various sources?
   - Standard authoritative data source translator
   - Sensor as a Service

Future State of Operator Environment

Providing the adaptive environment to include all the equipment, ingredients, and utensils for application developers to satisfy mission requirements.

While "under the covers", the future state:

- **Provides rapid provisioning of infrastructure &tools**
- **Better leverages of commercialized technology to support the warfighter**
- **Support's agile development of mission software providing user capabilities**

A fully stocked & instrumented kitchen for chef's to create their recipes

Questions?