# Operation Vulcan Logic - Agile Authorizations with Discipline

Daniel C. Holtzman, HQE
Director, Cyberspace Innovation (A);
Cyber Technical Director
04 August 2021

Authorizing Official for:
Cloud & DevSecOps;
F-35 Cloud & DevSecOps;
GBSD Cloud & DevSecOps
Command & Control Systems;
Rapid Cyber Acquisitions (RCA);
SAP Command & Control Systems;
SAP Rapid Cyber Acquisitions (RCA);
Enterprise IT as a Service (EITaaS);
SAP Enterprise IT as a Service (SEITaaS);

# Cyber Security Panel

## Moderator:

- **Mr. Daniel Holtzman, HQE**
  - Director, Cyberspace Innovation (A)

## Panel:

- **Ms. Lauren Knausenberger, SES**
  - DAF Chief Information Officer
- **Ms. Kristen Baldwin, SES**
  - Deputy assistant secretary of the Air Force for science, technology and engineering
- **Maj Gen Michael Schmidt, USAF**
  - PEO, C3I&N
- **Mr. Joe Bradley, SES**
  - Director, Cyber Resiliency Office for Weapon Systems

**LCID Theme: How is USAF adapting and influencing new acquisition business models in an ever changing environment?**

**Cyber Security Panel Questions:**

**What keeps you up at night regarding Cyber Security & Resiliency?**

**What are your top three Cyber Security & Resiliency Challenges?**

**What are your top three recommendations for the DAF with respect to Cyber Security and Resiliency?**

# Agenda

- **Areas of Responsibility**
- **AF Authorizing Official perspective**
- **Strategic Challenges / Initiatives**

*Be around the light bringers,*
*the magic makers,*
*the world shifters.*

*They challenge you,*
*break you open,*
*uplift and expand you.*

*They don't let you play small*
*with your life.*

*These heartbeats are your people.*
*These people are your tribe.*

*- Danielle Doby*

# Areas Of Responsibility (AOR)

## AF Cyber Technical Director AFLCMC/EN

Cyber Security Engineering and Resilience (CSER) Senior Leader;

Technical authority for:
- Security engineering, Cyber resiliency and systems and mission assurance;
- Engineering resilient systems;
- Defensive security engineering.

## AF Authorizing Official, SAF/CN

Authorization Boundaries:
- Cloud & DevSecOps;
- Command & Control Systems;
- SAP Command & Control Systems;
- Rapid Cyber Acquisition;
- SAP Rapid Cyber Acquisitions;
- Enterprise IT as a Service (EITaaS);
- SAP Enterprise IT as a Service (SEITaaS);
- F-35 Joint Strike Fighter (JSF), Cloud & DevSecOps;
- Ground Based Strategic Deterrent (GBSD), Cloud & DevSecOps.

## AF Director, Cyberspace Innovation, SAF/CN (Acting)

- Innovation thought leadership of risk-based cyber security across the DAF (USAF and USSF);
- Accelerate DAF understanding and mastery of commercial best practices;
- Collaboration across Government, Industry, Allies, and Partners ;
- Manage DAF technical standard setting and adoption process;
- Represent DAF/DoD interests in the international standard-setting process;

Data is current as of 01 May 2021

# AO Boundary – At A Glance
# Cross Section of Air Force Programs

CRC

- Wide Area Surveillance
- ShOC-N
- C2IMERA
- BACN
- TORCC / RADSIL

TAC-P


- JADC2 / ABMS
- Kessel Run / AOC
- Cloud One / Platform One
- E3 AWACS & JSTARS
- F-35 Cloud & DevSecOps
- GBSD Cloud & DevSecOps

cUAS

- PRC2
- WaRTAK
- GCCS / DCGS
- Pocket-J
- TBMCS
- Mission Planning
- Special Programs
- USAFE & PACAF

E-3


- ElTaaS & SElTaaS
- RDT&E DREN
- Commercial UAS
- NGAD

AOC

# Agenda

- **Areas of Responsibility**
- **AF Authorizing Official perspective**
- **Strategic Challenges / Initiatives**

*Cyber Security*

*&*

*Resiliency*

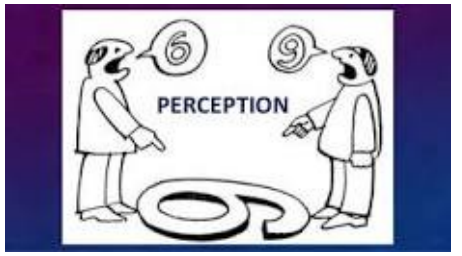
*Is a Journey,*

*Not a Destination*

*- D.C. Holtzman*

# Cultural - Unperceived Bias

- **“Cool, you 3D-printed the save icon!”**




**Two thirds of children don't know what a floppy disk is**

Children aged 6-18 were shown the photos below and asked if they knew what each was. Figures shown are the % of children who either said they didn't know what the item was, or gave an incorrect answer (children answered in their own words)


*Do you know the answer to these?*

*Do you realize your own Bias?*

*Communications is key to Culture change…….*

**Change your thoughts and you change your world.** ***– Norman Peale***

# AO Objectives
## An approach to Agile Risk Management

- **Objectives**
  - Make decisions faster - Transparent, Foster reciprocity
  - Facilitate risk management, - Acquisition, Operations & Sustainment
  - Enable Program Managers - Advance Cyber Security & Cyber Resiliency
- **Enablers**
  - Set Clear requirements – Sample Determination Briefing
  - Standard System Engineering - Evidentiary Analysis & Data based
  - Single AO for each Weapon System – Streamline expectations
  - Focus on risks that matter – Operational Focused with Enterprise view
- **Collaborative Execution**
  - Cyber Risk Assessors (CRA), (formerly SCA) focused on assessing risks
  - Authorizing Official  informs enterprise decision makers on Cyber Risks
  - Partnerships PEO's, DOEs, PMs, Users, Sustainers enables holistic view

**Increasing Decision Making Agility - Focus on Risk Management**

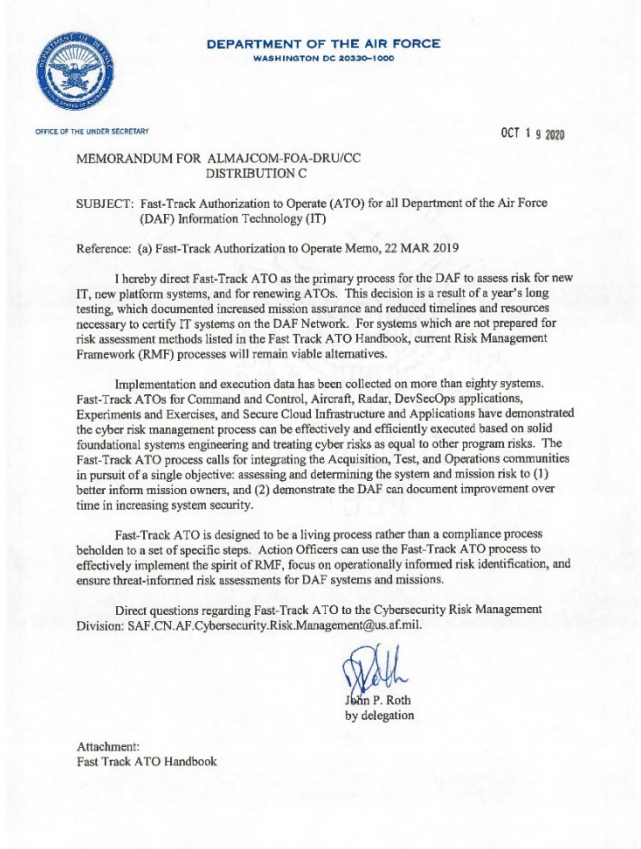
# Fast Track ATO Process
## What Is it?

- **Not a "New" process – Focus is on RISK Management**
- **Provides AOs ability to make RISK informed determinations – Spirit of RMF**
- **Does not require anything "New" or compliance to a new process**

**"The Fast-Track process gives Authorizing Officials (AOs) the discretion to make an authorization determination based on review of the combination of a Cybersecurity Baseline, an Assessment (e.g. Penetration Test), and an Information Systems Continuous Monitoring Strategy.**

**"AOs are expected to make operationally informed risk determinations by working closely with information systems owners and warfighters to find the appropriate balance between rapid deployment and appropriate level of risk assessment."**

- **Fast Track is <u>NOT Easy Button</u>, requires Robust Systems Engineering and Going Slow to go Fast**



DEPARTMENT OF THE AIR FORCE
WASHINGTON DC 20330-1000

OFFICE OF THE UNDER SECRETARY

OCT 19 2020

MEMORANDUM FOR ALMAJCOM-FOA-DRU/CC
DISTRIBUTION C

SUBJECT: Fast-Track Authorization to Operate (ATO) for all Department of the Air Force (DAF) Information Technology (IT)

Reference: (a) Fast-Track Authorization to Operate Memo, 22 MAR 2019

I hereby direct Fast-Track ATO as the primary process for the DAF to assess risk for new IT, new platform systems, and for renewing ATOs. This decision is a result of a year's long testing, which documented increased mission assurance and reduced timelines and resources necessary to certify IT systems on the DAF Network. For systems which are not prepared for risk assessment methods listed in the Fast Track ATO Handbook, current Risk Management Framework (RMF) processes will remain viable alternatives.

Implementation and execution data has been collected on more than eighty systems. Fast-Track ATOs for Command and Control, Aircraft, Radar, DevSecOps applications, Experiments and Exercises, and Secure Cloud Infrastructure and Applications have demonstrated the cyber risk management process can be effectively and efficiently executed based on solid foundational systems engineering and treating cyber risks as equal to other program risks. The Fast-Track ATO process calls for integrating the Acquisition, Test, and Operations communities in pursuit of a single objective: assessing and determining the system and mission risk to (1) better inform mission owners, and (2) demonstrate the DAF can document improvement over time in increasing system security.

Fast-Track ATO is designed to be a living process rather than a compliance process beholden to a set of specific steps. Action Officers can use the Fast-Track ATO process to effectively implement the spirit of RMF, focus on operationally informed risk identification, and ensure threat-informed risk assessments for DAF systems and missions.

Direct questions regarding Fast-Track ATO to the Cybersecurity Risk Management Division: SAF.CN.AF.Cybersecurity.Risk.Management@us.af.mil.

John P. Roth
by delegation

Attachment:
Fast Track ATO Handbook

**Fast Track is a philosophy of focusing on the Risk of Use, vice compliance**

# Cyber Security & Resiliency Enablers: First Step – Systems Engineering

1. What is the System? What does it do? CONOPS? Missions?
2. What is the System Architecture? Weapon System (e.g. Aircraft, Ground Systems, Maintenance systems, Training systems……)
3. List of Hardware (LRU), Software and providence of each (e.g. supply chain); identification of Critical Program Information (CPI), Critical Components (CC); Technical Orders, Operational procedures. Identification of technologies being used.
4. Identification of all external communications access points
5. How does Data flow into, thru and out of the system? What type of data? How is it protected? Where does it come from? Where does it go? What is it used for?
6. What Threat/Intel information is available?

**Establish baseline from Known data**

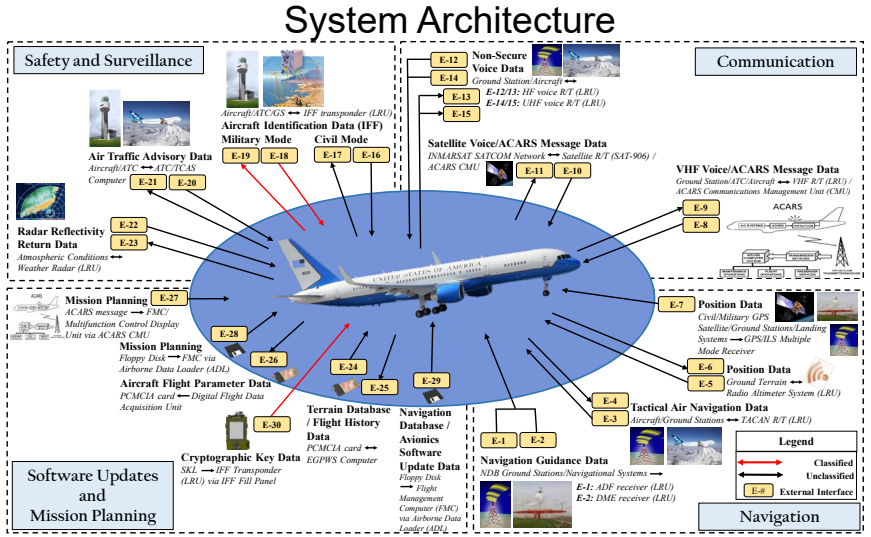
# Cyber Security & Resiliency Enablers: First Step – Systems Engineering

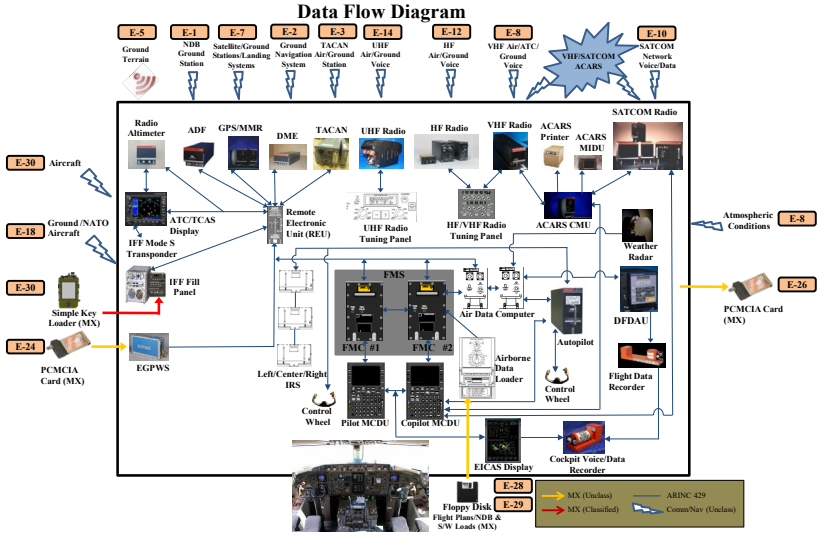
1. **Bill of Material (BOM) - As part of the SE process, especially in a legacy system, programs already know all parts (HW and SW);**
2. **Existing supplier management process identifies source of suppliers, End of Life (EOL) analysis, and alternate part analysis. (Document "As Is")**
3. **Existing criteria being used by primes and flowed down to subs, on purchasing of parts is known?**
4. **What is the supply chain mapping? Does one exist already?**
   - **Graphically representation of supply chain down?**

- **With the data collected from item 1-4 above - review of potential RISKS of the supply chain can be done rather quickly at low cost – "As Is/Known"**
- **Available intel/ threat info can be applied against the list of parts or suppliers identified (or technologies) – If Known**
- **Provides an assessment of risk of the current supply chain**
  - **Better than we have today**

**Establish baseline from Known data**

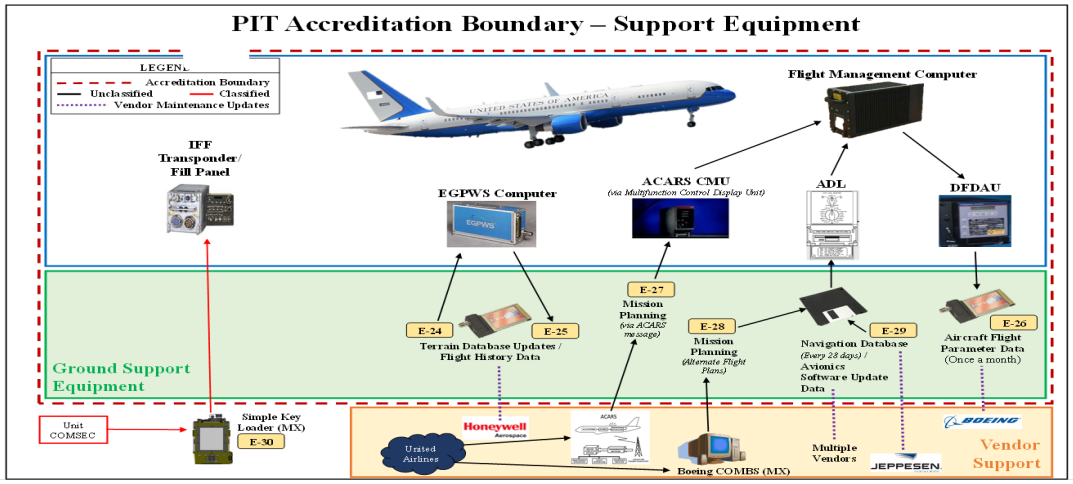
# Weapon System Views: Understanding the Authorization Boundary




*Understand the Risk of Use*

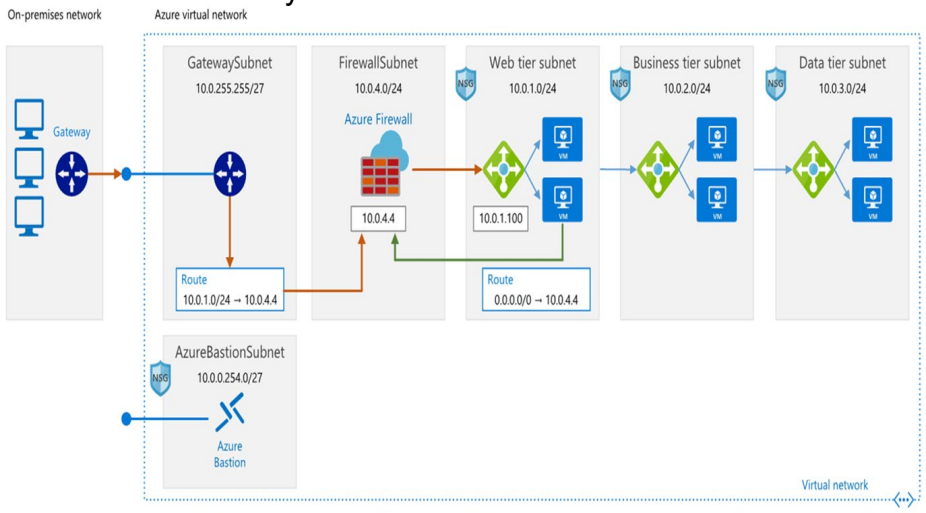
*Focus on Risk Management in Operational Context*




*Systems Engineering Evidentiary Data & Analysis based*

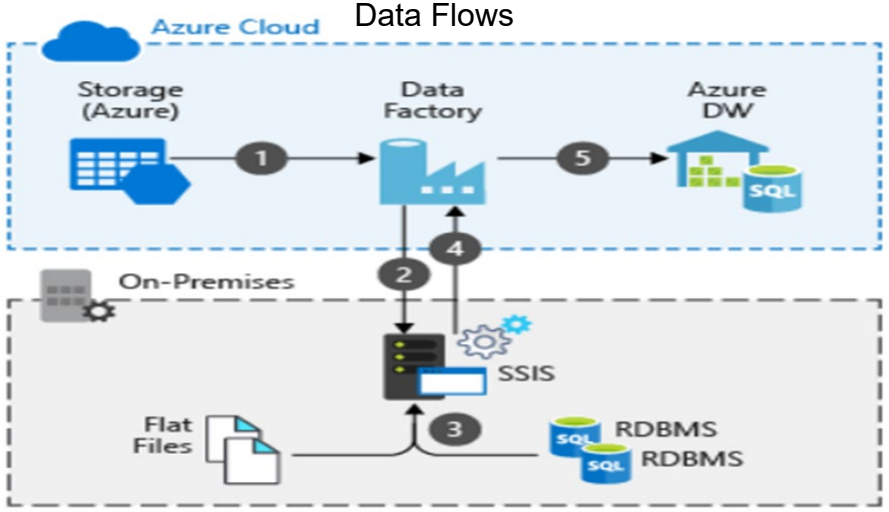
# Cloud Environment Views: Understanding the Authorization Boundary

## System Architecture

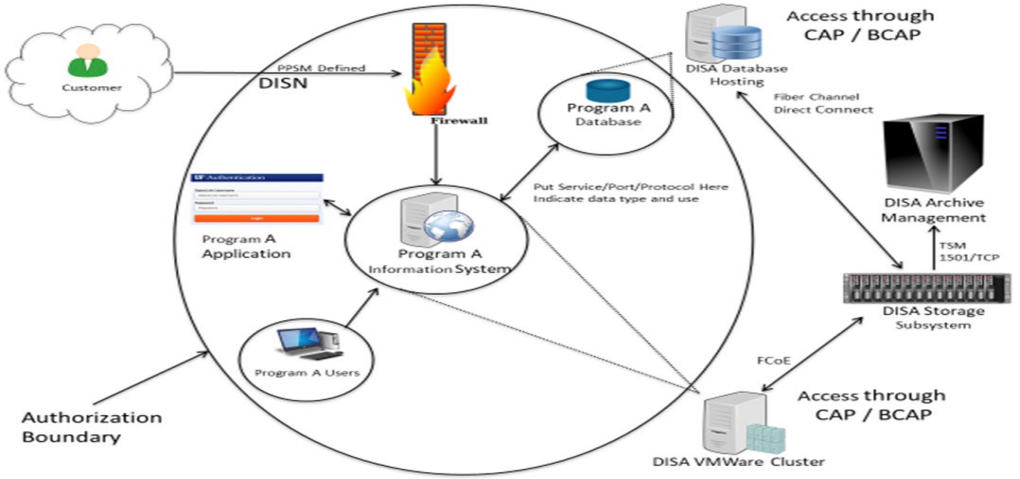



- CSSP services include but are not limited to:
  - External Vulnerability Scans (EVS)
  - Web Vulnerability Scanning (WVS)
  - Malware Notification Protection (MNP)
  - Support and Training (S&T)
  - Network Security Monitoring (NSM)
  - Attack Sensing & Warning (ASW)
  - Warning Intelligence (WI)
  - Incident Reporting (IR)
  - Incident response Support (IRS)
    - Volatile Data Analysis (VDA)
    - Forensic Media Analysis (FMA)
    - Reverse Engineering and Malware Analysis (RE/MA)
    - Cyber Hunt/Intrusion Assessment (IA)
    - Incident Response (IR)
  - Sustainment & Configuration Management (SCM)
  - HBSS or DoD approved equivalent Anti-Virus
  - Port Whitelisting through DISA

## Data Flows




## Authorization Boundary



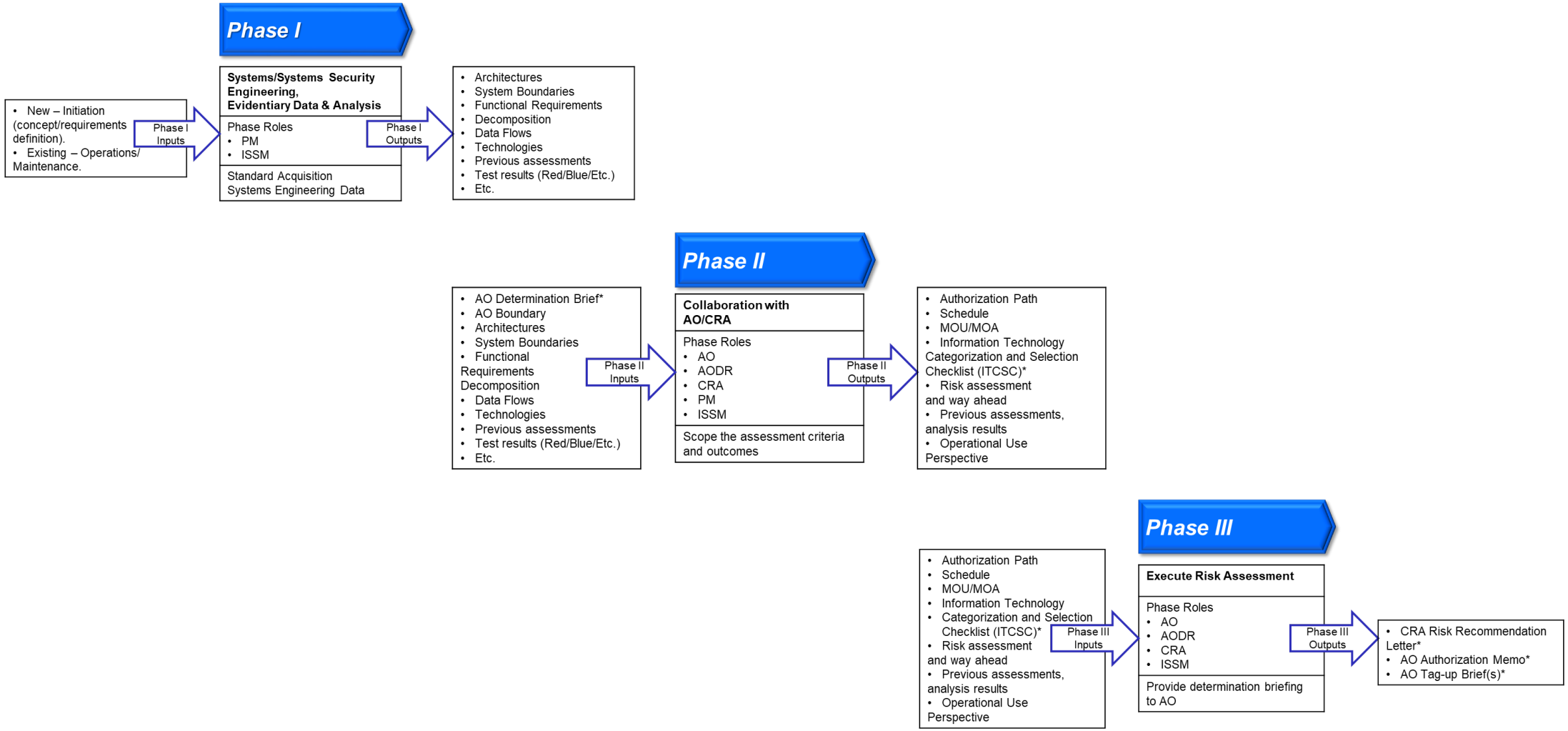
# Agile Authorizations Risk Based View

| Phase I | Phase II | Phase III |
|---|---|---|
| **Grow it In** | | |
| Systems/Systems Security Engineering<br>Evidentiary Data & Analysis | Collaboration with AO/CRA | Execute Risk Assessment |
| • Architectures<br>• System Boundaries<br>• Functional Requirements Decomposition<br>• Data Flows<br>• Technologies<br>• Previous assessments<br>• Test results (Red/Blue/Etc.)<br>• Etc. | • Discuss risk assessment and way ahead<br>• Previous assessments, analysis results<br>• Operational Use Perspective | • Tool Agnostic – Focus on Evidentiary Data and Analysis<br>• Clinically define Risk of Use Posture<br>• Outline Mitigations for Risks |
| Standard Acquisition Systems Engineering Data | Scope the assessment criteria and outcomes | Provide determination briefing to AO |

**The Program Manager is empowered to participate in the determination process and own the actions in the POA&M**

Daniel C. Holtzman, HQE

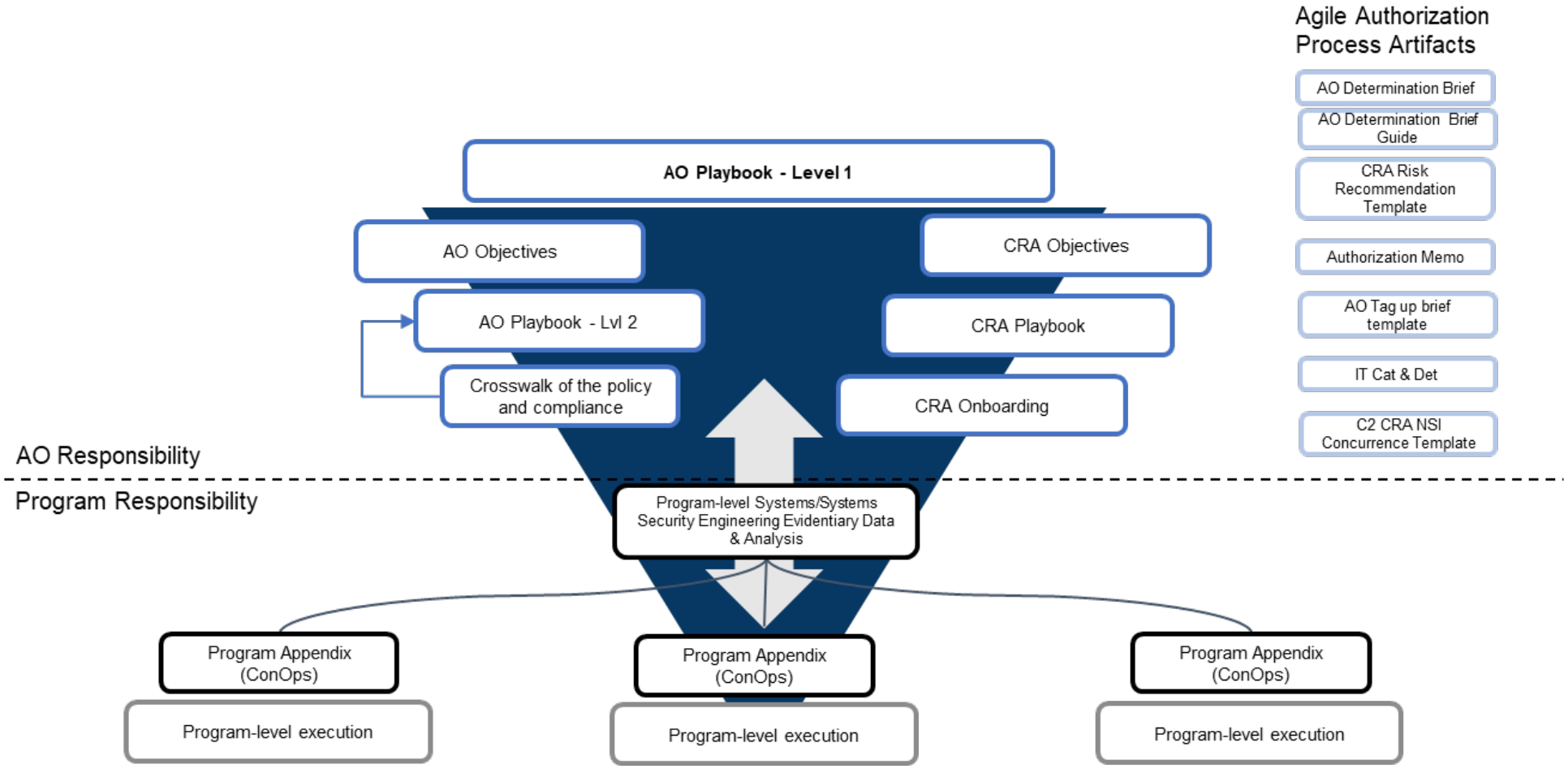
# Agile Authorizations
# Disciplined Systems Engineering






Daniel C. Holtzman, HQE

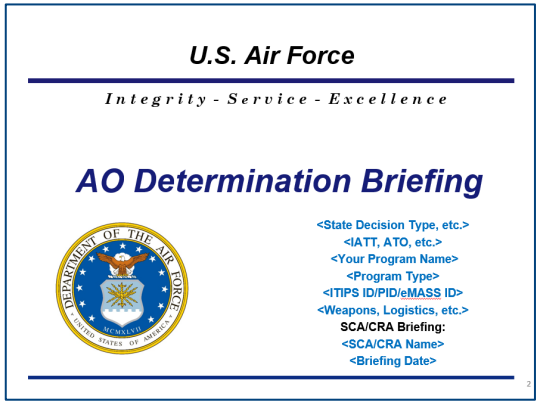
# Operation Vulcan Logic
# Agile Authorizations Execution NorthStar




**Holistic, Continuous Authorization Ecosystem: Focused on Risk or Use**

# Agile Authorizations: Templates & Guides

- **Determination Brief**

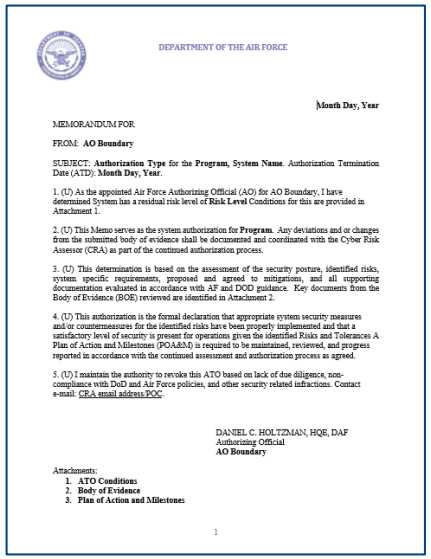

U.S. Air Force

Integrity - Service - Excellence

AO Determination Briefing

<State Decision Type, etc.>
<IATT, ATO, etc.>
<Your Program Name>
<Program Type>
<ITIPS ID/PID/eMASS ID>
<Weapons, Logistics, etc.>
SCA/CRA Briefing:
<SCA/CRA Name>
<Briefing Date>

- **Authorization Memo**


DEPARTMENT OF THE AIR FORCE

Month Day, Year

MEMORANDUM FOR

FROM: **AO Boundary**

SUBJECT: **Authorization Type** for the **Program, System Name**. Authorization Termination Date (ATD): **Month Day, Year.**

1. (U) As the appointed Air Force Authorizing Official (AO) for AO Boundary, I have determined System has a residual risk level of **Risk Level** Conditions for this are provided in Attachment 1.

2. (U) This Memo serves as the system authorization for **Program**. Any deviations and or changes from the submitted body of evidence shall be documented and coordinated with the Cyber Risk Assessor (CRA) as part of the continued authorization process.

3. (U) This determination is based on the assessment of the security posture, identified risks, system specific requirements, proposed and agreed to mitigations, and all supporting documentation evaluated in accordance with AF and DOD guidance. Key documents from the Body of Evidence (BOE) reviewed are identified in Attachment 2.

4. (U) This authorization is the formal declaration that appropriate system security measures and/or countermeasures for the identified risks have been properly implemented and that a satisfactory level of security is present for operations given the identified Risks and Tolerances A Plan of Action and Milestones (POA&M) is required to be maintained, reviewed, and progress reported in accordance with the continued assessment and authorization process as agreed.

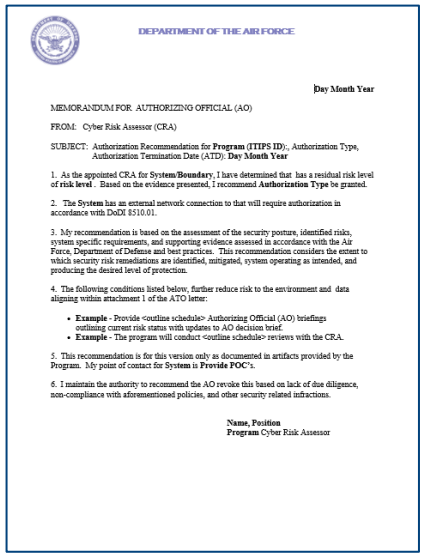
5. (U) I maintain the authority to revoke this ATO based on lack of due diligence, non-compliance with DoD and Air Force policies, and other security related infractions. Contact e-mail: CRA email address/POC.

DANIEL C. HOLTZMAN, HQE, DAF
Authorizing Official
**AO Boundary**

Attachments:
1. **ATO Conditions**
2. **Body of Evidence**
3. **Plan of Action and Milestones**

1

- **CRA Risk Recommendation**


DEPARTMENT OF THE AIR FORCE

Day Month Year

MEMORANDUM FOR AUTHORIZING OFFICIAL (AO)

FROM: Cyber Risk Assessor (CRA)

SUBJECT: Authorization Recommendation for **Program (ITIPS ID)**:, Authorization Type, Authorization Termination Date (ATD): **Day Month Year**

1. As the appointed CRA for **System/Boundary**, I have determined that has a residual risk level of risk **level** . Based on the evidence presented, I recommend **Authorization Type** be granted.

2. The **System** has an external network connection to that will require authorization in accordance with DoDI 8510.01.

3. My recommendation is based on the assessment of the security posture, identified risks, system specific requirements, and supporting evidence assessed in accordance with the Air Force, Department of Defense and best practices. This recommendation considers the extent to which security risk remediations are identified, mitigated, system operating as intended, and producing the desired level of protection.

4. The following conditions listed below, further reduce risk to the environment and data aligning within attachment 1 of the ATO letter:

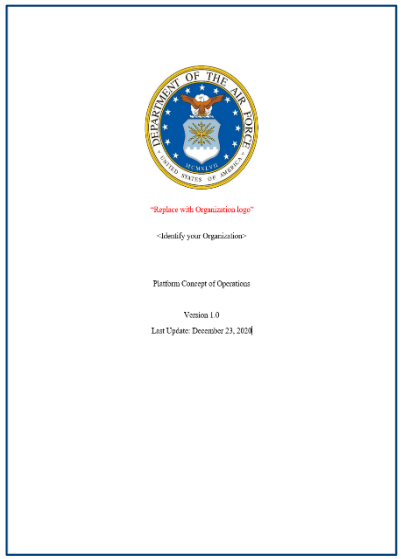
- **Example** - Provide <outline schedule> Authorizing Official (AO) briefings outlining current risk status with updates to AO decision brief.
- **Example** - The program will conduct <outline schedule> reviews with the CRA.

5. This recommendation is for this version only as documented in artifacts provided by the Program. My point of contact for **System** is **Provide POC's**.

6. I maintain the authority to recommend the AO revoke this based on lack of due diligence, non-compliance with aforementioned policies, and other security related infractions.

**Name, Position**
**Program** Cyber Risk Assessor

- **DevSecOps Conops (as applicable):**


"Replace with Organization logo"

<Identify your Organization>

Platform Concept of Operations

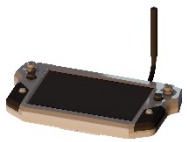
Version 1.0

Last Update: December 23, 2020

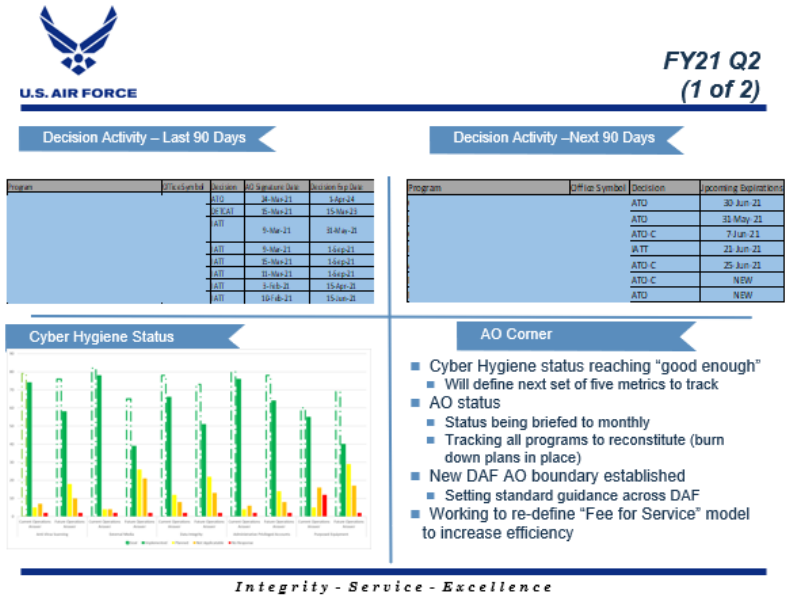
**Flexible standardization for authorization packages.**
**There is no one size fits all approach.**

# AF Fast Track Process Exemplar
# US Government Wide Reciprocity

- **Defense Innovation Unit (DIU) Initiative**
  - **SAF/CN AF Focal Point**
- **Reciprocity for GSA Schedule**
  - **Navy worked two cUAS**
  - **AF worked Three cUAS, using Fast Track Process**
    - **ATOs provided and cUAS are on GSA Schedule**
    - **All other cUAS removed from GSA Schedule**
- **Objective:**
  - **Apply AF Fast Track Process to Enable Reciprocity**
  - **Short Term - Vet cleared COTS UAS for GSA Schedule**
  - **Long Term – SAF/CN, SAF/AQ, HAF/A3, HAF/A2, HAF/A5/8 Engaged**

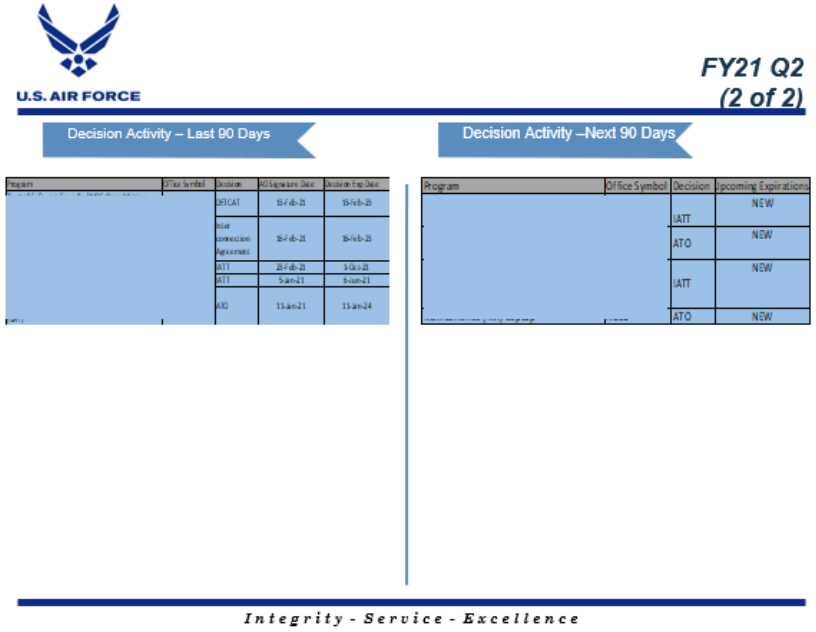



# PEO Updates
## An AO / PEO Partnership




- **PEO AODR assigned**
  - **Works for PEO DOE**
  - **OPCON to AO**
  - **Integrates Cyber into SE/SSE**
- **PEO AODRs collect Metrics and status**
- **Quads are available on PEO Dash Boards**

- **AO to PEO Quarterly Update**
  - **Communicate Status**
    - **Set Expectations**
- **Cyber is Commanders Business**



# Risk Adjudication Process: Cyber is Commanders Business

- **Authorizing Official (AO) Determines Risk is High**
- **AO Communicates with Program Manger (PM)**
  - **Agree and mitigate = Stop here**
- **AO & PM jointly present to PEO**
  - **Agree and Mitigate = Stop here**
- **AO & PEO present to Risk Board**
- **Risk Board: CIO, SAE, System Operational Commander**
- **Risk Board Weighs Risk, Tolerance, Mission and Enterprise**

**Risk of Use is communicated to:**
**Acquisition, Enterprise and Operational Stakeholders**

# Collaborative Partnerships

- **AF CSO, CAO, CEO, CDO, CIO – Strategic Alighment**
- **Air Force and Space Force Collaborations**
- **AF Authorizing Officials**
  - **Weapon Systems AOs - Reciprocity agreement in place**
  - **AFRL AO - Collaborating on Fast Track ATO & Reciprocity**
  - **HAF/A4 AO - Collaboration and Reciprocity**
  - **AF Innovation AO - Collaboration on SecDevOps and Cloud migration**
  - **AF Global Strike Command – Collaborating on Reciprocity**
  - **Enterprise AO - Reciprocity across boundary**
  - **AF IC AO – Collaboration on Reciprocity – ADSV exemplar**
  - **16th AF AO – Collaboration on Reciprocity & AO process**
  - **AF OSI/PJ – Collaboration on Reciprocity, sharing of resources**
  - **DOD CIO – Reciprocity agreement in place**
- **Industry**
  - **Collaboration via AF/Industry Authorization Round Table**
- **External Agencies**
  - **NSA, National Nuclear Security Agency (NNSA), DHS, DLA, USDA, Army RCO, Army NETCOM, DOJ, Navy, Others …….**

- **Agile Execution based on Collaborative partnerships Vice Policy and Memos**
- **Building Confidence and Trust**

# Agenda

- **Areas of Responsibility**
- **AF Authorizing Official perspective**
- **Strategic Challenges / Initiatives**

*The most dangerous phrase in*

*language is*

*"We've always done it*

*this way".*

*- Admiral Grace Hopper*

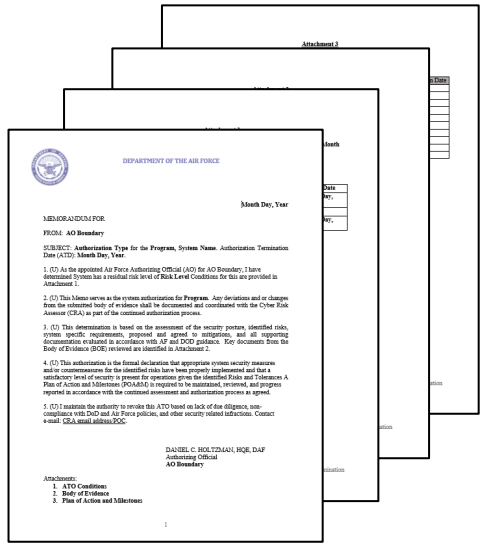
# Strategic Challenges

- **Reciprocity**
  - **The Myth of lowest common denominator**
- **Culture of Compliance**
  - **Compliance Masquerading as Risk Management**
- **Operational Risk integration**
  - **Risk is Temporal & Context Sensitive**
- **Command & Control**
  - **Too Many Cooks makes for bad tasting Chili**

**Cyber is Commanders Business**

# ATO Package of the future

- **Will Document the Key items needed for Reciprocity**
- **Authorization Memo**
- **Attachment 1 – Conditions**
- **Attachment 2 – Body of Evidence**
  **Attachment 3 – Plan of Action and Milestones**




- **Attachment 1 – Conditions**
  - **Documents any Conditions on the ATO**
  - **Security is a journey, never a destination**
  - **Includes Risk of Use Label to inform the Consumer**
- **Attachment 2 – Body of Evidence**
  - **Key artifacts that supported the authorization**
  - **Informs other AOs and Consumers to increase Reciprocity**
- **Attachment 3 – Plan of Action and Milestones**
  - **Classified Appendix**

# Authorization Determination Types

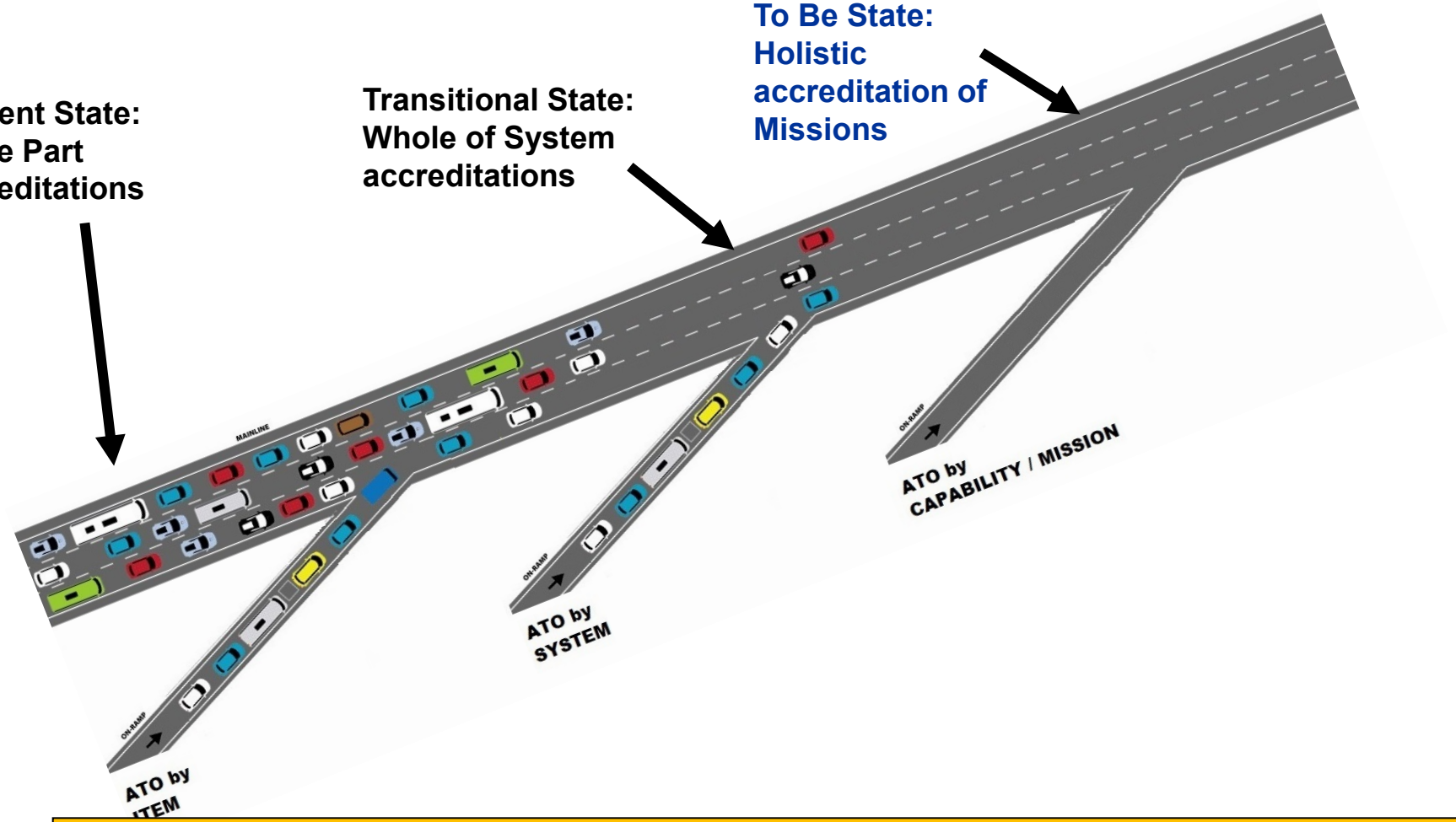
| Authorization Type | Authorization Details | Required Artifacts |
|---|---|---|
| ATO | The risk to organizational operations, organizational assets, individuals, other organizations, and the Nation is acceptable. | • AO Determination Brief<br>• CRA Risk Recommendation<br>• Assessment Reports(s)<br>• Plan of Action and Milestones<br>• IT Categorization and Selection Checklist |
| ATO With Conditions (ATO-C) | The risk to organizational operations, organizational assets, individuals, other organizations, and the Nation is acceptable, but conditions exist. | • AO Determination Brief<br>• CRA Risk Recommendation<br>• Assessment Reports(s)<br>• IT Categorization and Selection Checklist<br>• Plan of Action and Milestones |
| Continuous ATO (c-ATO) (c-ATO will be applied to DevSecOps pipelines ONLY) | Accredits the platform and process and certifies team that produces a product under a continuous monitoring process that maintains the residual risk within the risk tolerance of the Authorizing Official (AO). | • AO Determination Brief<br>• CRA Risk Recommendation<br>• Conops: platform, process, and teams.<br>• IT Categorization and Selection Checklist |
| IATT | Operational environment or live data is required to complete specific test objectives. | • AO Determination Brief<br>• CRA Risk Recommendation<br>• IT Categorization and Selection Checklist<br>• Certification Test Plan |
| Authorization to Use (ATU) | AO acceptance of risk in using cloud or shared services (system, service, or application) chooses to accept the system, service, or application in an existing authorization package produced by another organization. Authorization to use is a mechanism to promote reciprocity for systems under the purview of different AOs, based on a need to use shared systems, services, or applications. | • Official AO authorizing letter from the originating organization.<br>• Existing authorization package and deployment instructions produced by originating organization, where appropriate. |
| Certificate to Field (CtF) | Trustworthiness ensures no risks exist, either of malicious or unintentional origin. Predictable execution ensures there is a justifiable confidence that software, when executed, functions as intended. | • CRA Risk Recommendation<br>• USAF Scan Load Scan Checklist |
| DATO | The information system is not authorized to operate. | • DATO Memo |

# Highway to Resilient Capabilities

**Current State:**
**Piece Part accreditations**

**Transitional State:**
**Whole of System accreditations**

**To Be State:**
**Holistic accreditation of Missions**




*Moving Towards Agile Authorizations*

*Understand the Risk of Use of the System in the context*

*Focus on the Risk Management in Operational Context*

**Traditional Boundary configuration management is no longer sufficient in a Software defined, ubiquitous connected environment**

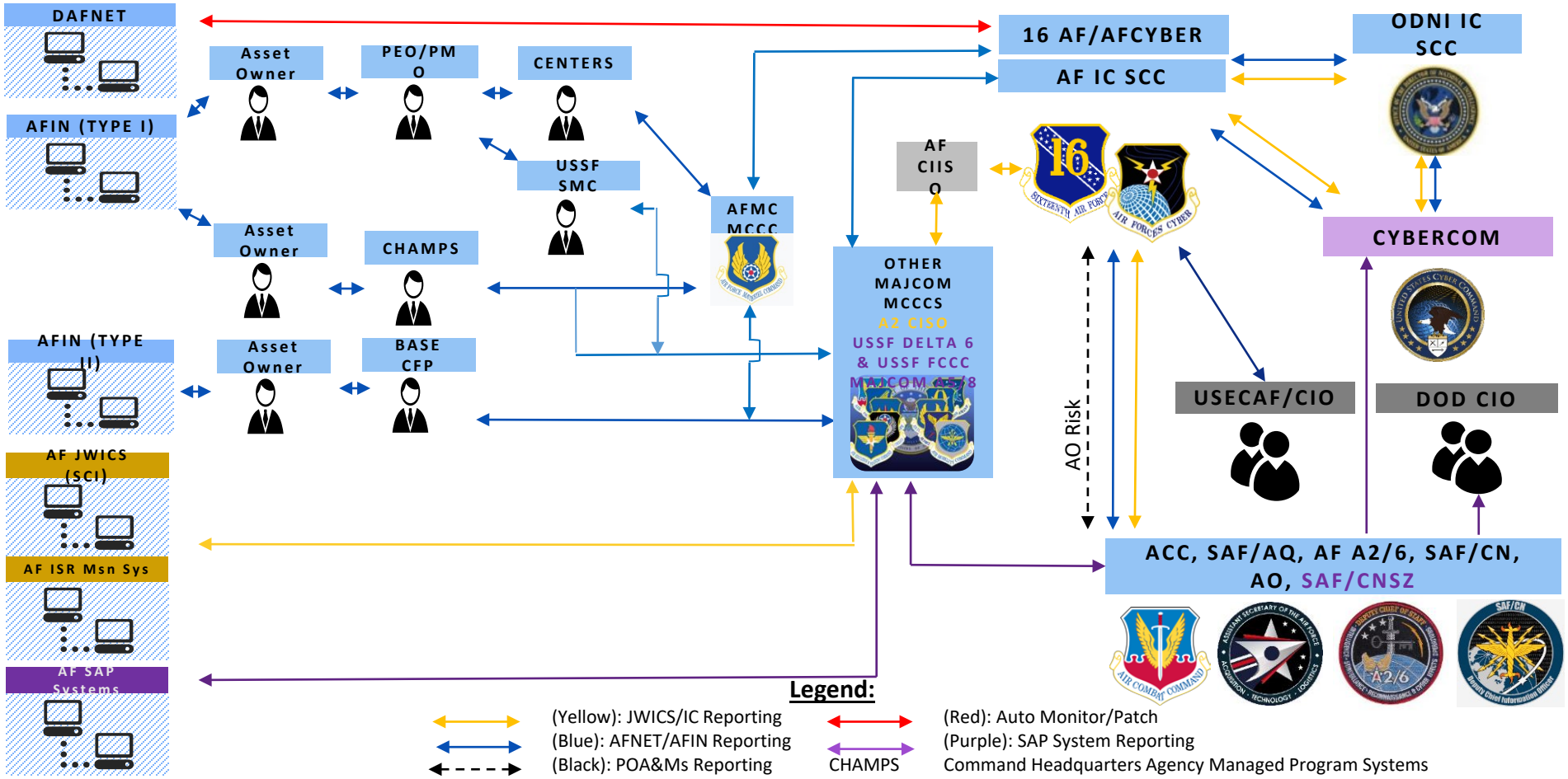
# eMASS Guidance

- **The Program Manager's: {per AFI 17-101}**
  - **Ensures Cybersecurity and Resilience requirements, attributes, and design consideration are designed into newly acquired systems and modified systems**
  - **Ensure that programs meet statutory regulatory & system Requirements**
  - **Balance lifecycle cost, schedule, system performance, risk, and system security**
  - **Required to register all IT in the appropriate eMASS instance**
  - **Required to upload to eMASS (at minimum):**
    - **IT Categorization and Selection Checklist**
    - **Cybersecurity Strategy**
    - **Authorization Memo**
- **Authorizing Official {Per AFI 17-101}**
  - **Render authorization determination balancing mission needs & security concerns in my boundary**
  - **Authorization Determination is in eMASS**

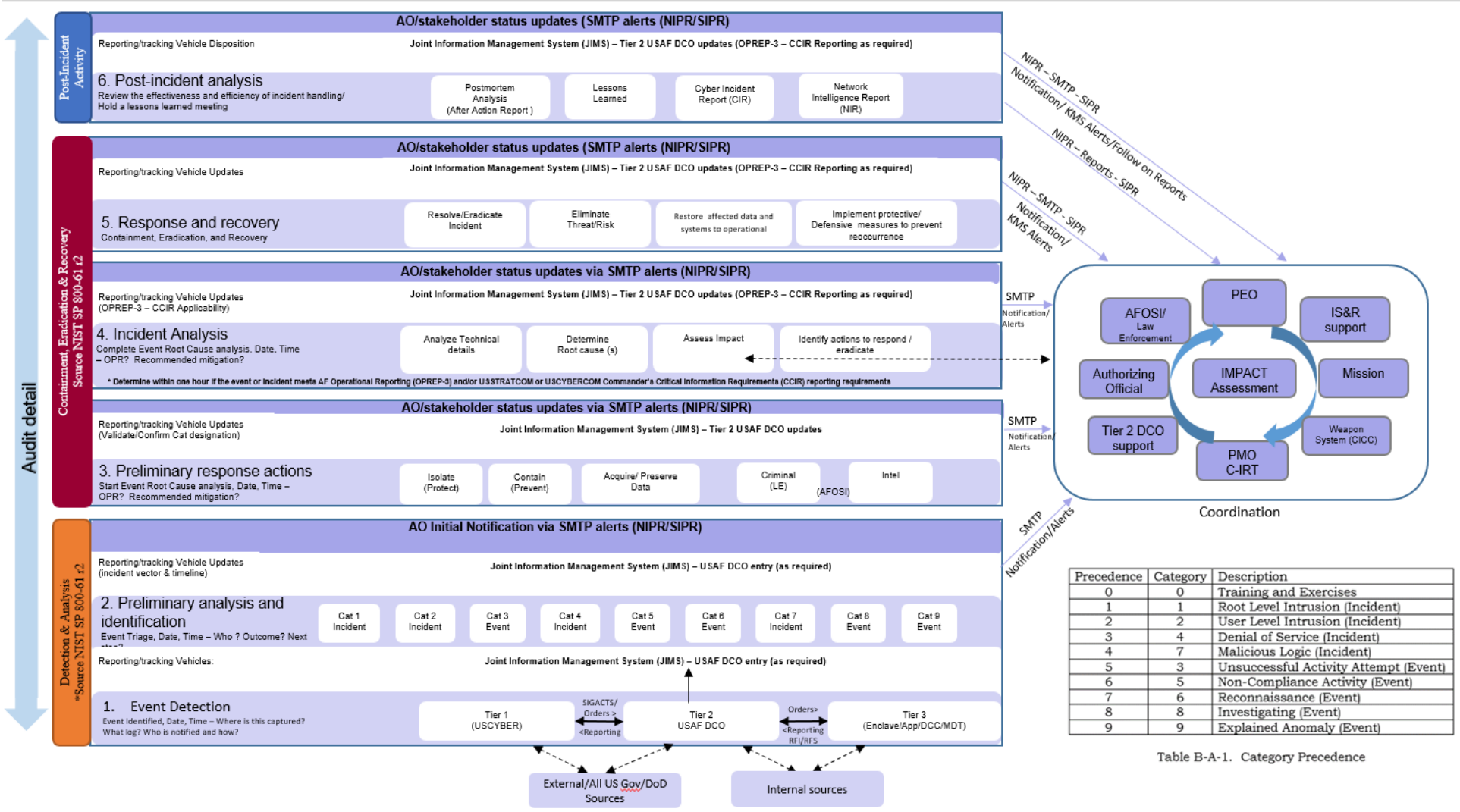
# eMASS Guidance

- **Cybersecurity Risk Assessors (CRA)s {Per specific boundary requirements}**
  - **Assess IT and provide a risk recommendation including:**
    - **Draft ATO Memo**
    - **CRA Recommendation Memo**
      - **Risk analysis report**
      - **IT Categorization and Selection Checklist**
      - **DevSecOps Concept of Operation (Conops) {If Applicable}**
    - **Determination Brief**
  - **Validate controls in eMASS to support reciprocity and assist with uploading authorization package as needed**

# Operation Spartan Wizard
# Cyber Operations Communications Model



# Outlining Incident Response Criteria




| Precedence | Category | Description |
|---|---|---|
| 0 | 0 | Training and Exercises |
| 1 | 1 | Root Level Intrusion (Incident) |
| 2 | 2 | User Level Intrusion (Incident) |
| 3 | 4 | Denial of Service (Incident) |
| 4 | 7 | Malicious Logic (Incident) |
| 5 | 3 | Unsuccessful Activity Attempt (Event) |
| 6 | 5 | Non-Compliance Activity (Event) |
| 7 | 6 | Reconnaissance (Event) |
| 8 | 8 | Investigating (Event) |
| 9 | 9 | Explained Anomaly (Event) |

Table B-A-1. Category Precedence

# Cyber Tech Order & Continuous Monitoring

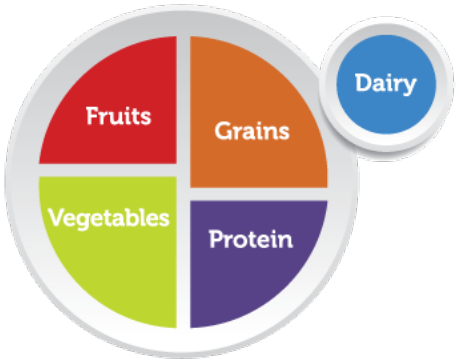
- **Cyber Tech Order**
  - **Communicate the "How" to maintain Systems for Secure Resiliency**
  - **Provide clear operating instructions for Users and Maintainers**
  - **Educate, Enable and Execute**
- **Continuous Monitoring**
  - **Recognition that change is constant**
    - **New vulnerabilities, threats every day**
    - **Technology changes**
    - **Mitigation effectiveness degradation over time**
  - **Integration of Mission Defense Teams into CONMON plans**
    - **First line of defense**

| | |
|---|---|
| 1. | **Executive Abstract (1 to 2 explanatory paras per bullet – 2 pages max)** |
| | • Secure and Resilient System Design Overview |
| | • Secure and Resilient Operations Overview |
| | • Secure and Resilient System Sustainment Overview |
| 1. | **ATO Compliant Execution (3 paras no more than 1 page + 1 page docs reference table)** |
| | • Managing Operations in Accordance with the System Security Plan |
| | • Actions or behaviors that can impact the ATO |
| | • Reference Documentation |
| 1. | **Training & Awareness (Will engage SSR for applicable training references)** |
| | **3.1 - Statement that Unit level ISSM/ISSO/ Security Officer/ COMSEC Officer responsible for ensuring training and awareness of entire unit.** |
| | 3.2 - Conducting Periodic System/Network Operations Secure Practices Training |
| 1. | **Configuration Control & Patching (typically an introductory line or two referencing any mandated policy followed by practical tips guiding implementation. Will utilization of Top level instruction and guidance for outlining the unit's responsibility – same format for remaining sections)** |
| | 4.1 - Maintaining Configuration Baselines |
| | 4.2 - Updating for Malicious Code Protection (anti-virus/malware; code patches; GPOs, TCNOs, TCTOs, etc.) |
| | 4.3 - Performing Configuration and Change Management |
| 1. | **Controlling Identity and Access Management** |
| | **(Top level Statement with Unit level Security Officer/ISSM/ Info Owners having first step of responsibility with Physical/Data SAAR access)** |
| | 5.1 - Limiting Access to Authenticated Entities |
| | 5.2 - Controlling System Access Requirements |
| | 5.3 - Controlling Internal & Remote System Access |
| | 5.4 - Controlling and Limiting Physical & Remote Data Access |
| | 5.5 - Controlling and Limiting Data Access to only Authorized Users and Processes |
| 1. | **Managing Information** |
| | 6.1 - Controlling Communications at System Boundaries (PPS / NOSC / etc.) |
| | 6.2 - Protecting Auditing/Monitoring Information |
| | 6.3 - Managing Backups |
| | 6.4 - Identifying and Marking Media |
| | 6.5 - Protecting and Controlling Media Storage and Transport |
| | 6.6 - Sanitizing & Destroying Media |
| 1. | **Continuous Auditing/Monitoring** |
| | 7.1 - Auditing/Monitoring Requirements |
| | 7.2 - Configuring Auditing/Monitoring for Systems and Networks |
| | 7.3 - Cyber Health Auditing/Monitoring |
| | 7.4 - Reviewing and Managing Auditing Logs and Monitoring Tools |
| | 7.5 - Monitoring Threats |
| 1. | **Incident Response and Reporting** |
| | 8.1 - The NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover) |
| | 8.2 - Conducting Incident Response Training Exercises |
| | 8.3 - Identifying Risks and Protecting Capabilities and Services |
| | 8.4 - Detecting and Responding to Incident and Events |
| | 8.5 - Reporting a Potential or Declared Incident or Event |
| | 8.6 - Recovering from an Incident or Event |
| | 8.7 - Performing Post Incident/Event Reviews |

# Cyber Risks Facts Label Concept

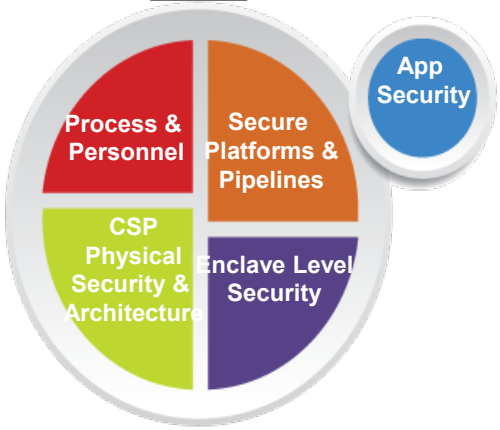
- **Application Security is NOT just about the security of the application itself**
  - **It is a layered perspective (Hosted environment, TTPs, etc.)**
  - **As one goes lower in an application architecture, potential for harm increases**
- **An Authority to Operate (ATO) is a Risk based Determination, which includes many factors:**
  - **Technology employed, Execution processes, Hosting Environment, Risk tolerance, etc.**
  - **The ATO is a statement of "Risk of Use" – to inform the consumer**

**Food**



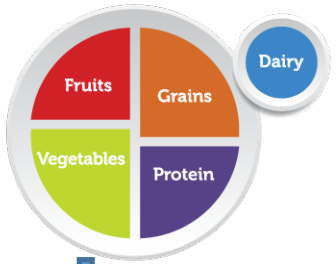

**Just like a well-balanced meal, Risk is made up of several ingredients**

**ATO**




**Cyber Risk is made up of several ingredients**

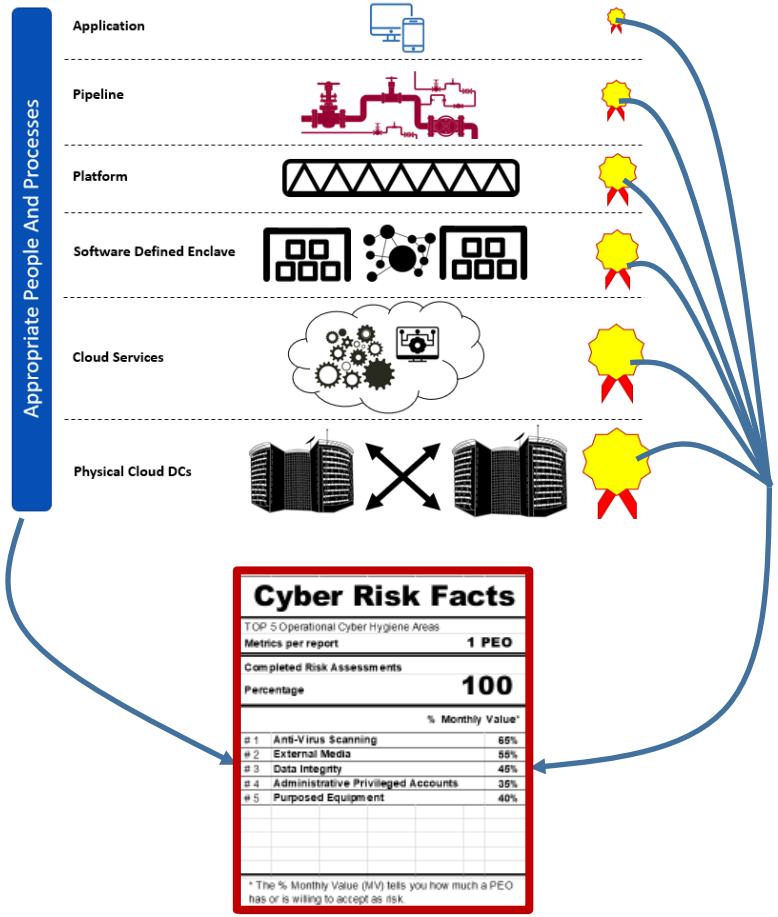
# Cyber Risk Facts Label
# Allowing For An Informed Consumer





- **A Nutritional Facts Label shows the consumer WHAT nutrients are in the food based on FDA guidelines**

- **A Cyber Risk Label shows the consumer WHAT the Risk of Use is for an application based on ATO Guidelines**




**Cyber Risk label is the foundational to an informed consumer and enabling true reciprocity**

Daniel C.
Holtzman, HQE

# Cloud & DevSecOps AO Summit

**3-4 November 2020**

# A Joint Air Force & Space Force Collaboration

Hosted by
Mr. Daniel C. Holtzman, HQE, DAF

Daniel C. Holtzman, HQE

# Joint AF / SF Cloud & DevSecOps AO Summit
## Bottom Line Up Front

- **To hear from the Field**
- **To understand where you think we are**
- **To hear your Thoughts on the way forward**
- **To Enable the Light bringers**

**What keeps you up at night regarding Cyber, Cloud & DevSecOps?**

**What are your top 3 Cyber Challenges with Authorizations in Cloud & DevSecOps?**

**What are your top 3 recommendations for the AF with respect to Authorizations in Cloud & DevSecOps?**

**Coming Together is a Beginning;**
**Keeping Together is Progress;**
**Working Together is Success.** *- Henry Ford*

Daniel C.
Holtzman, HQE

# Summary Keys to Success

- **Assurance**
  - **Establish Confidence:**
    - **That we have assessed all the most significant risks**
    - **Authorizations are not the finish line**
    - **Continuous Monitoring is key enabler**
- **Reciprocity**
  - **Establish Trust:**
    - **Reciprocity is about Trust…we will be transparent**
    - **Risk tolerance variance is expected**
- **Partnership**
  - **Establish Collaborative Risk Assessments**
    - **Early coordination with other stakeholders is Key to success**
    - **PEOs, SML/ML/PM, Other AOs, Other stakeholders (ATEA, TSN), Users (ACC), Industry, AFRL**
    - **Fast Track ATO is key enabler**


**This is a work in progress….Need to continue to collaborate**

# AFRMFKS Published AO Boundary Document Descriptions

- **AO Determination Brief Template**
  - **Brief to assist program personnel in understanding what the Authorizing Official is expecting to see to make an informed risk determination.**
- **AO Determination Brief Guide**
  - **An AO determination brief guide has also been created to provide guidance on the completion of the above AO determination brief.**
- **AO Defined Roles & Responsibilities Chart**
  - **Roles and responsibilities for key stakeholders the AO or AO staff will interact with**
- **AO Playbook**
  - **A high-level guide on the AO objectives with Criteria, Observables, and Behavior (COB) expectations and templates used when interacting with the Authorizing Official for authorization determinations.**
- **AO Tag-up Brief Template**
  - **Used to provide regular updates on system status to allow the Authorizing Official or Designated Representative to make continuous and on-going, risk-based determinations based on guidance from the Authorizing Official.**
- **AODR/CRA Appointment Letter Template**
  - **Is used to ensure personnel are directly appointed, in writing, to the roles of an AODR or CRA**
- **Authorization Memo Template**
  - **Leveraged to articulate the authorization determination to stakeholders. After the determination of risk from the operation or use of the information system has been made, this letter is used to inform the System Owner and other stakeholders of the authorization determination along with terms and conditions for the authorization.**

# AFRMFKS Published AO Boundary Document Descriptions

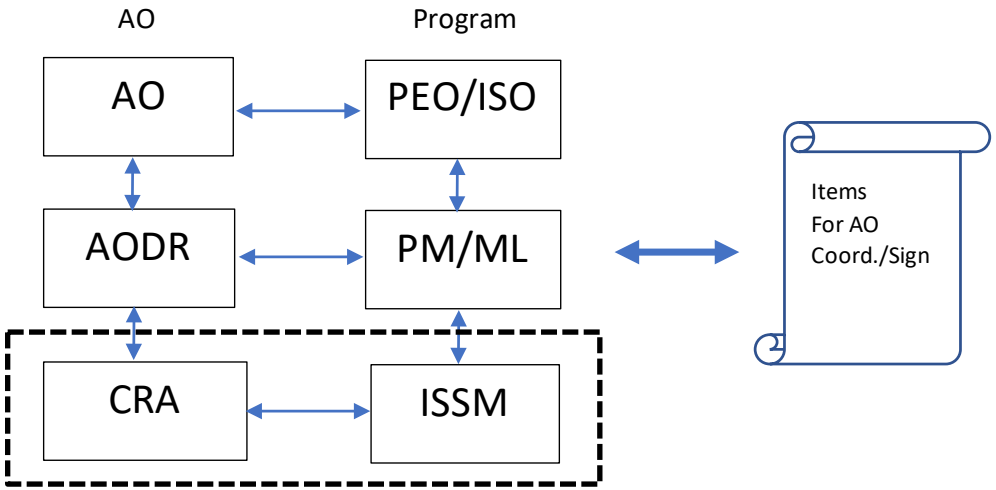
- **CRA Objectives –**
  - **Overall CRA goals and basic introduction to the Fast-Track Agile Authorization process (Key steps/documents)**
- **CRA Onboarding –**
  - **Introduction/definition of the tools (documents), websites, Roles and Responsibilities, engineering phases/outputs, documentation workflow etc.… what the CRA needs to be successful in meeting the objectives/goals.**
- **CRA Playbook**
  - **Outlines the Agile Authorization Process, Objectives , step by step approach along with the templates used when interacting with the AO for authorization decisions.**
- **CRA Risk Recommendation Letter**
  - **The document the CRA uses to articulate the risk recommendation once the risk assessment is complete.**
- **DSOP ConOps**
  - **Addresses the process flows of developed code and software and the people that perform duties within that process flow and covers the Hardware/Software and the people that operate the infrastructure.**
- **Information Technology Categorization and Selection Checklist (ITCSC) –**
  - **Form to document the security categorization of the system, including the information processed by the system and represented by the identified information types.**
- **No Security Impact (NSI)**
  - **The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system.**

# AFRMFKS Published AO Boundary Doc Links

| | Title | Role | Responsibilities (AO-Defined) |
|---|---|---|---|
| **System Owners** | Program Executive Officer (PEO) | Senior Acquisition Official | Responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of a System/Capability. |
| | Information System Owner (ISO) | System Operational Owner | Responsible for system requirements definition, funding advocacy, system acceptance, system employment, and operations. |
| **Assess and Authorize** | Authorizing Official (AO) | Authorizing Official | Responsible for assessing and determining the Risk of Use for the System or Capability and informing the System/Capability stakeholders. Provides Authorizations to Operate (ATOs) with specific guardrails, assumptions, constraints, and acceptable risk tolerance. |
| | Authorizing Official Designated Representative (AODR) | AO Designated Representative | Represents the AO in all matters as outlined by the AO. |
| | Cyber Risk Assessors (CRA) | Independent Risk Assessor | Responsible for providing the AO with an independent Cyber Risk Analysis and acceptable Risk of Use for the System or Capability. |
| **Acquisition Program** | Information System Security Manager (ISSM) | Program/Capability Cyber Lead | Responsible for integration of cybersecurity into and throughout the lifecycle of the System or Capability as the cybersecurity technical advisor to the PM and/or the ISO. |
| | Program Manager (PM) | Program/Capability Manager | Responsible for the System/Capability development and delivery. Responsible for registering System/Capability in the ITIPS, eMASS, or similar authorization tracker and for obtaining an ATO from an AO. |

# Cyber Team Comms Flow

- **Below is a list of typical items that require AO signature or attention and the path to successful coordination (samples only):**
  - **IT Categorization: ISSM -> PM/ML -> ISSM -> SCA/CRA -> AODR (if delegated, signed here) ->AO**
  - **Risk Assessment: ISSM -> SCA/CRA + PM/ML, SCA/CRA (if No security impact) if new authorization creates determination briefing, body of evidence, and memorandum(s) follow determination briefing path.**
  - **Determination Briefing: ISSM -> SCA/CRA -> AODR -> AO (ISSM notifies within Program office chain status of determinations (need dates, If package is high risk coordinate with PM/ML-> PEO/ISO, etc.)**



# CRA Training Agenda

- **Module 0: Authorizing Official's (AO) Perspective**
  - Mr. Holtzman
- **Module 1: Fast Track**
  - What is it?
  - Background
  - Elements
  - Fast Track and RMF
  - Authorization Determinations
- **Module 2: Authorizing Official (AO)**
  - Introduction
  - Roles and Responsibilities
  - AODR's
  - AO Objectives, Enablers and Collaboration
  - AO Playbook v1.0
- **Module 3: Cyber Risk Assessor (CRA)**
  - Introduction
  - CRA Responsibilities
  - CRA Objectives v1.0
  - CRA Onboarding v1.0
  - CRA Playbook v1.0
- **Module 4: Body of Evidence, Artifacts - Information Tools**
  - *AO Determination Brief
  - AO Determination Brief Guide
  - *CRA Recommendation Letter
  - *DevSecOps (DSOP) CONOPs (If applicable)
  - *Draft AO Authorization Letter
  - *IT Categorization and Selection (ITCSC)
- **Module 5: CRA Assessments**
  - In/Out Briefing
  - Assess Only Process
  - Security Assessment Plan (SAP)
  - Risk Assessment Report (RAR)
  - Security Assessment Report (SAR)
  - Plan of Action & Milestone (POA&M)
  - Authorization Determination Package (Minimal Requirements)
- **Module 6: Continuous Execution**
  - Continuous Monitoring Plan (ConMon)
  - Conditions/ Residual Risks
  - Sustainment and Maintenance
  - No Security Impact (NSI)
  - STIGs and Scans
  - Risk Assessment Report
  - Reciprocity
  - Repository (eMASS/Xacta etc.)
- **Module 7: Agile Authorization Ecosystem**
  - Putting all of this together
  - Phased Approach
  - Risk Based View
  - Disciplined Systems Engineering Workflow
  - Agile Authorization Artifacts
  - Summary

* Key AO Information

# Questions & Discussion


**Operation Vulcan Logic**

AIR FORCE LIFE CYCLE MANAGEMENT CENTER