Cyber Risk Assessor (CRA) Onboarding

Daniel C. Holtzman
Authorizing Official (AO)
DOD Chief Digital & Artificial Office (CDAO)

Authorizing Official for:
DOD CDAO;
JSF F-35 ALIS.

Aug 2023

CDAO

Agenda

- **Module 0: Authorizing Official's (AO) Perspective**
  - Mr. Holtzman Introduction Video
- **Module 1: Fast Track**
  - What is it?
  - Background
  - Elements
  - Fast Track and RMF
  - Authorization Determinations
- **Module 2: Authorizing Official (AO)**
  - Introduction
  - AODR's
  - Cyber Team Roles and Responsibilities
  - AO/CRA Communication
  - AO Objectives, Enablers and Collaboration
  - AO Playbook v1.0
- **Module 3: Cyber Risk Assessor (CRA)**
  - Introduction
  - CRA Roles and Responsibilities
  - CRA Objectives v1.0
  - CRA Onboarding v1.0
  - CRA Playbook v1.0

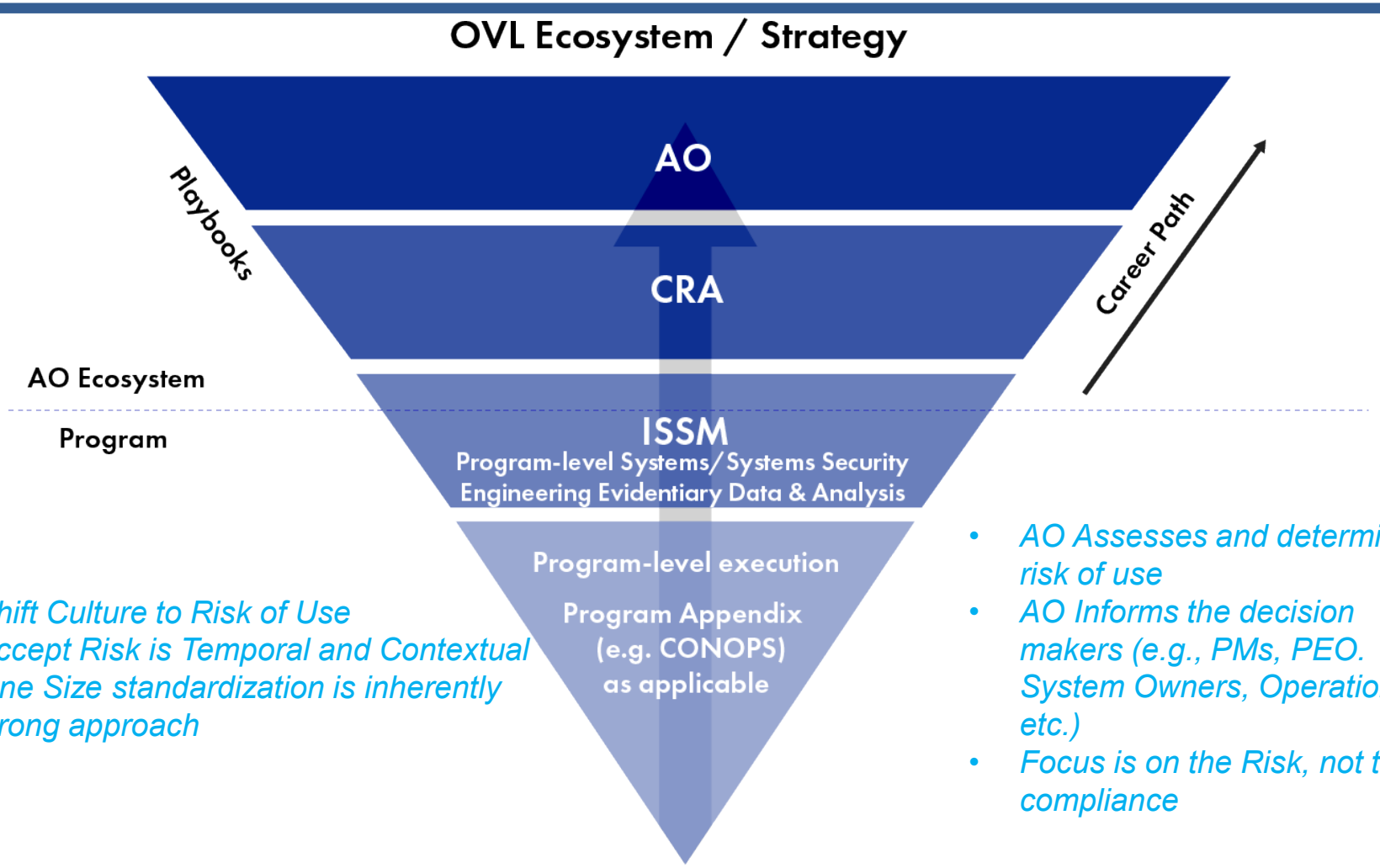
* Key AO Information

- **Module 4: Body of Evidence, Artifacts - Information Tools**
  - * IT Categorization and Selection Checklist (ITCSC)
  - * AO Determination Brief
  - * Risk Analysis Report
  - * CRA Recommendation Letter
  - * Draft AO Authorization Letter
  - * Risk Assessment Report
  - DevSecOps (DSOP) CONOPs (If applicable)
  - AO Determination Brief Guide
  - Documentation A&A Lifecycle
- **Module 5: CRA Assessments**
  - Assess Only Process
  - Security Assessment Plan (SAP)
  - Risk Assessment Report (RAR)
  - Security Assessment Report (SAR)
  - Plan of Action & Milestone (POA&M)
  - In/Out Briefing
- **Module 6: Continuous Execution**
  - Continuous Monitoring Plan (ConMon)
  - Conditions/ Residual Risks
  - No Security Impact (NSI)
  - Reciprocity
  - eMASS
- **Module 7: Agile Authorization Ecosystem**
  - Putting all of this together
  - Phased Approach
  - Summary

Module 0

Authorizing Official's (AO) Perspective

Operation Vulcan Logic: Agile Authorizations Execution NorthStar



- *Shift Culture to Risk of Use*
- *Accept Risk is Temporal and Contextual*
- *One Size standardization is inherently wrong approach*

- *AO Assesses and determines risk of use*
- *AO Informs the decision makers (e.g., PMs, PEO. System Owners, Operations, etc.)*
- *Focus is on the Risk, not the compliance*

The holistic, continuous authorization ecosystem is focused on Risk of Use.

Module 1

Fast Track

Fast Track - What is it?

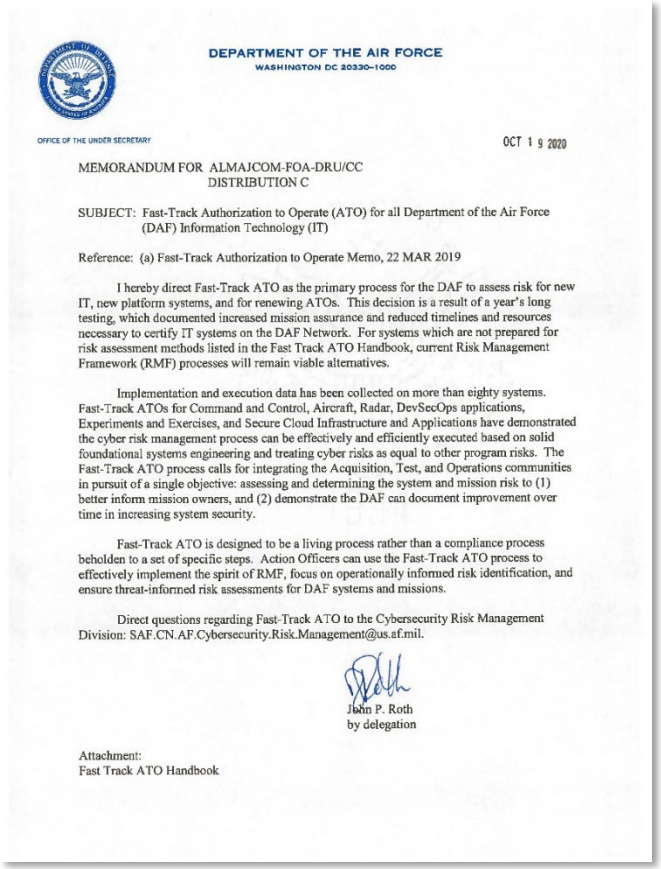
- Simple approach to rendering an authorization.
  - Introduces the "Agile Authorization Process", think Assessment and Authorization Process
- Streamlined to fully comply with Risk Management Framework's (RMF) intent
- Focus on "RISK" vice "COMPLIANCE"
- Provides AOs the ability to make "Risk-based" determinations
- "Does not" remove/replace requirements to comply with Federal Mandates
- "Applications for Fast Track include developed software for secured cloud infrastructures, but AOs may consider other applications as well."

Fast-Track ATO Process: What Is It?

- **Not a "new" process: Focus is on risk management and complies with DOD 8510.**
- **Provides AOs the 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 [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.*"



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 <u>NOT an "easy" button</u>; It requires robust systems engineering and "going slow to go fast."**

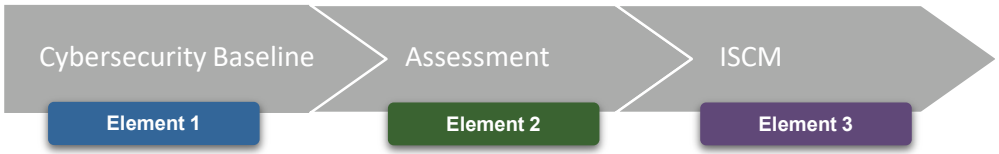
Fast-Track is a philosophy of focusing on the Risk of Use vs. Compliance Only.

Fast Track ATO – Elements

- ***Fast Track ATO process applies to all systems and boundaries*** to maintain the specified timelines and to prove the system is built and maintained securely.

- Fast Track ATO utilizes core functions of the Cybersecurity Framework (CSF) along with selected RMF controls to manage risk and prioritize the assessment of demonstrable cybersecurity in an operationally relevant environment.

  - **Element 1: Cybersecurity Baseline**
    - Implement a baseline that is aligned with Cybersecurity Framework (CSF) and FISMA reporting metrics
  - **Element 2: Assessment**
    - System subjected to assessment/validation.
  - **Element 3: Information Systems Continuous Monitoring (ISCM) Strategy**
    - Ensure the system is monitored continuously for changes that may introduce new vulnerabilities or elevated risks
    - Continuous monitoring must be assessed annually



U.S. AIR FORCE
Fast Track ATO

OVL and RMF

OVL	RMF
Phase 1: Systems/Systems Security Engineering Evidentiary Data & Analysis	Step 0: Prepare
	Step 1: Categorize
	Step 2: Select Security Controls
	Step 3: Implementation of the Security Controls
Phase 2: Collaboration with AO/CRA	Step 4: Assess Controls
	Step 5: Authorize System
Phase 3: Continually Execute Risk Management	Step 6: Monitor Controls

Authorization Determination Table

Authorization Type	Authorization Details	Documentation
ATO	The risk to organizational operations, organizational assets, individuals, other organizations, and the Nation is acceptable.	• AO Determination Brief • AO Authorization Memo • CRA Risk Recommendation • Plan of Action and Milestones • IT Categorization and Selection Checklist • Reference: Supporting Evidence
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 • AO Authorization Memo • CRA Risk Recommendation • Plan of Action and Milestones • IT Categorization and Selection Checklist • Reference: Supporting Evidence
Continuous ATO (c-ATO) (Applied to DevSecOps 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 • CRA Risk Recommendation • CONOPs: platform, process, and teams. • IT Categorization and Selection Checklist • Reference: Supporting Evidence
IATT	Operational environment or live data is required to complete specific test objectives.	• AO Determination Brief • CRA Risk Recommendation • IT Categorization and Selection Checklist • Certification Test Plan • Reference: Supporting Evidence
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.	• AO Determination Brief • CRA Risk Recommendation • Plan of Action and Milestones • IT Categorization and Selection Checklist • Reference: Supporting Evidence
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.	• AO Determination Brief • CRA Risk Recommendation • Plan of Action and Milestones • IT Categorization and Selection Checklist • Reference: Supporting Evidence
DATO	The information system is not authorized to operate.	• DATO Memo

Questions

- What does Fast Track Introduce?
- What does Fast Track focus on?
- What are the 3 elements?

Module 2

AO Introduction, Objectives and Playbook

AO Introduction

- AOs are appointed positions within business and mission owner organizations.
- Render authorization decisions for Cloud Environments, DoD ISs and PIT systems under their purview in accordance with DoDI 8510.01.
- Responsible for authorizing or denying the operation (or the testing) of the assigned DoD information system by issuing an authorizing determination (i.e., ATO, IATT, DATO).
- Reviews the security authorization package, including accompanied by supporting material and the recommendation of the CRA as a basis for determining risk to provide an authorization determination.
- Assesses and determines the final "Risk of Use" for the system or capability *based on the evidence provided*.
- Informs the stakeholders of the outcome and determines guardrails, assumptions, constraints, and conveys acceptable risk tolerance levels.

Authorizing Official Designated Representative

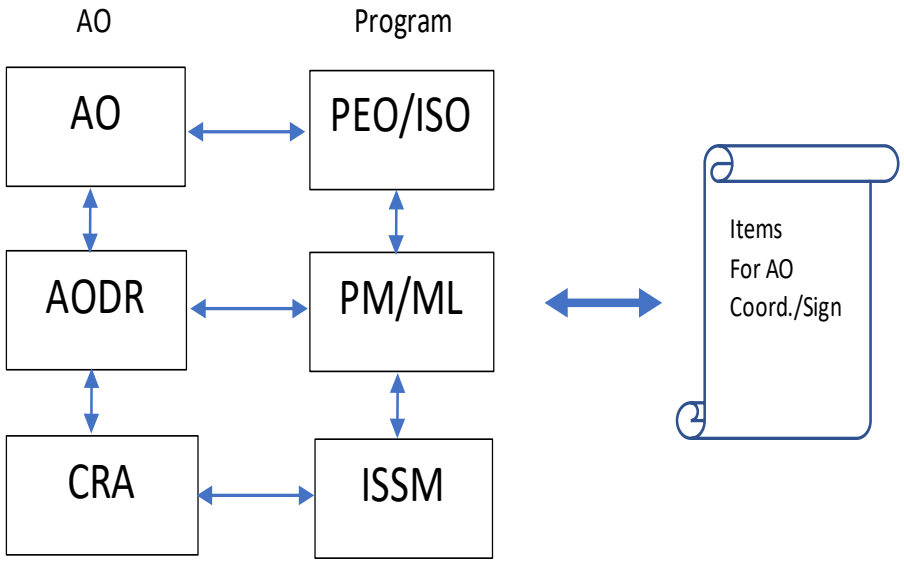
Scope of Responsibilities	PEO AODR	Boundary AODR
Can be empowered by authorizing officials to make certain decisions about the planning and resourcing of the security authorization process, approval of the security plan, approval and monitoring the implementation of plans of action and milestones, and the assessment and/or determination of risk.	X	X
May also be called upon to prepare the final authorization package, obtain the authorizing official's signature on the authorization decision document, and transmit the authorization package to appropriate organizational officials.	X	X
What cannot be delegated to the designated representative by the AO is the authorization decision and signing of the associated authorization decision document (i.e., the acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation).	N/A	N/A
Perform as the cyber risk assessor (CRA) or formally delegate the security control assessment role (representatives) for governed information technologies.	X	X
Identify and recommend changes and improvements to the security assessment process, security T&E, and risk assessment methodology, including procedures, risk factors, assessment approach, and analysis approach.	X	X
Track the assessment and authorization status of IS and PIT systems governed by the DoD Component cybersecurity program.	X	X
Establish and oversee a team of cybersecurity professionals qualified in accordance with DoDI 8570.01 responsible for conducting security assessments. DoD Component AODRs may task, organize, staff, and centralize or direct assessment activities to representatives as appropriate. Regardless of the adopted model, the DoD Component AODR is responsible for assessing quality, capacity, visibility, and effectiveness.	X	X
Advise AOs on the adequacy of acquisition program implementation of cybersecurity requirements.	X	X
Serve as the single cybersecurity coordination point for joint or Defense-wide programs that are deploying information technologies to DoD Component enclaves.	X	X

Cyber Team Roles and Responsibilities

FUNCTION	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 & operations.
Assess & 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 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/ 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 Manager / ML	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 Authorization to Operate 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.)



Note* Maintain open communications amongst the entire team!

AO/CRA Communication

AO Determination Briefing - Provides a concept of operations, defines the environment and requirements and a path to considering the intent and type of authorization Determination (i.e., IATT, ATO w/Conditions, etc.).

CRA Recommendation Letter - Defines the results from the formal Security Assessment, outlining all vulnerability and weaknesses found and defining recommended conditions for the program to follow in correcting each found item.

DRAFT Authorization Letter - A formal written statement by the Authorizing Official regarding the risk associated with operating the information system (IS) and expressed as an authorization to operate (ATO), interim authorization to test (IATT), or denial of ATO (DATO) etc.

IT Categorization and Selection Checklist (ITCSC) - Process of determining the security category for information or an information system. This checklist helps in determines impact values: (i) for the information type(s) processed, stored, transmitted, or protected by the information system; and (ii) for the information system and identify overlays that apply to the information system and its operating environment to account for additional factors (beyond impact) that influence the selection of security requirements.

DSOP CONOPs* (If applicable) - 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.

AO Objectives, Enablers and Collaboration

- **Objectives:**
  - Render decisions faster: Being Transparent, foster reciprocity;
  - Enable Program Managers: More Secure Tomorrow than today;
  - Facilitate risk management: Acquisition, operations, and sustainment.

- **Enablers:**
  - Setting clear expectations: AO Determination Briefing
  - Base Risk on Evidentiary analysis and data: Use Standard System Engineering:
  - Focus on Risk of Use: Operational-focused with enterprise view.
  - Move to Single AO for each system type (e.g., Cloud, DSOP, SAP, Weapons): Streamline expectations & Seams.

- **Collaborative Execution:**
  - Cyber Risk Assessors (CRA) (formerly SCA) focus on assessing risks;
  - Authorizing Official informs decision makers on cyber risks;
  - Partnerships with PEOs, DOEs, PMs, users, and sustainers enable holistic view.

Increase decision-making agility by focusing on risk management.

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

- What is the system? What does it do? CONOPS? Missions?
- What is the system architecture? Weapon system (e.g., aircraft, ground systems, maintenance systems, training systems, etc.)?
- List hardware (LRU) and software and the providences of each (e.g., supply chain); identify Critical Program Information (CPI), Critical Components (CC); technical orders, and operational procedures. Identify technologies being used.
- Identify all external communications access points.
- How does data flow into, through, 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?
- What threat/intel information is available?

Establish the baseline from known data.

Cyber Security & Resiliency Enablers: Supply Chain Risks

- Bill of Material (BOM) - As part of the Systems Engineering process, especially in a legacy system, programs already know all parts (HW and SW);
- Existing supplier management process identifies source of suppliers, End of Life (EOL) analysis, and alternate part analysis. (Document "As Is")
- Existing criteria being used by primes and flowed down to subs, on purchasing of parts is known ?
- What is the supply chain mapping? Does one exist already?
  - Graphical representation of supply chain down?
- With the data collected from item 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 the baseline from known data.

AO Playbook

- **Hold the AO to the Playbook**
- High-level guide on the Criteria, Observables and Behavior (COB) expectations and templates used when interacting with the AO for authorization determinations.
- Objectives, Enablers and Collaborative Execution
- Its "not" a magical formula – it's a "**Risk Based"** View
  - Standard Acquisition Systems Engineering Data
  - Scoping the assessment criteria and outcomes
  - Completing and providing a detailed Determination Briefing to the AO

Operation Vulcan Logic
Fast Track Implementation: Agile Authorizations

1 PHASE

Systems/Systems Security Engineering Evidentiary Data & Analysis

- Architectures
- System Boundaries
- Functional Requirements Decomposition
- Data Flows
- Technologies
- Previous Assessments
- Test Results (Red/Blue/Etc.)

Standard Acquisition Systems Engineering Data

Grow it in

PROGRAM MANAGEMENT

- Facilitate Risk management across S&T, Acquisition, Operations & Sustainment

2 PHASE

Collaboration with AO/CRA

- Discuss risk assessment and way ahead
- Previous assessments analysis results
- Operational Use Perspective

Scope the assessment criteria and outcomes

COLLABORATIVE EXECUTION

- Partnerships with PEO's, DOEs, PMs, S&T, T&E, Sustainers, Users, enables holistic view

3 PHASE

Continually Execute Risk Management

- Tool Agnostic - Focus on Evidentiary Data and Analysis
- Clinically define Risk of Use Posture
- Outline Mitigations for Risks

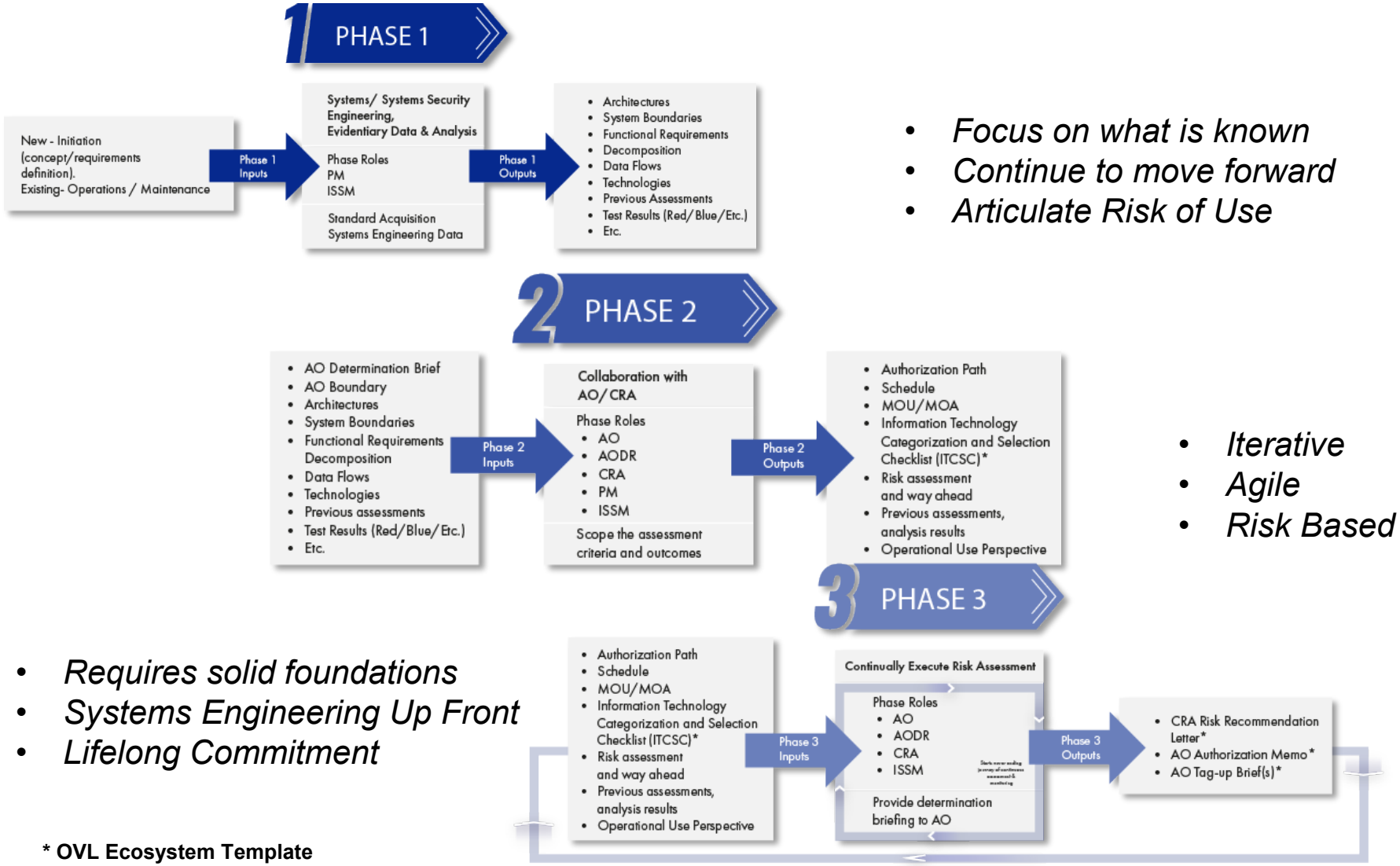
Starts never ending journey of continuous assessment & monitoring

ENABLERS

- Single, Lead AO for each Weapon System
- Streamline expectations and increase Agility

Operationalizing the Fast Track ATO Process

Agile Authorizations: Enabled by Disciplined Systems Engineering



- *Focus on what is known*
- *Continue to move forward*
- *Articulate Risk of Use*

- *Iterative*
- *Agile*
- *Risk Based*

- *Requires solid foundations*
- *Systems Engineering Up Front*
- *Lifelong Commitment*

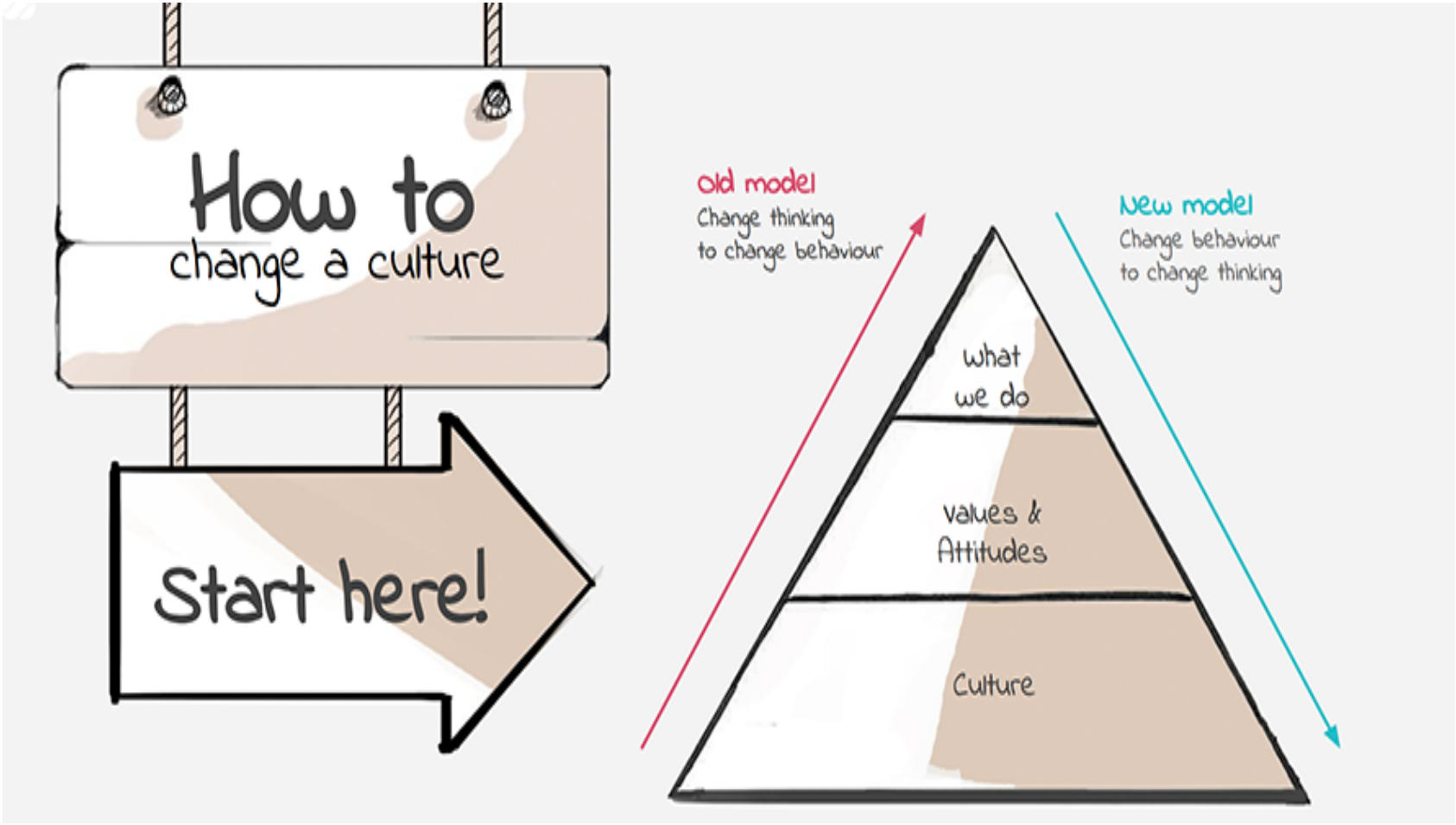
*** OVL Ecosystem Template**

Questions

- What is an Authorizing Official?
- What is the one thing an AODR cannot do?
- What responsibility does the CRA have?
- What role specifically keeps the AO in the loop?
- What are the 5 artifacts the CRA will use to communicate with the AO?
- What is the AO's first enabler? Why?
- Why is Supply Chain important?
- What does the AO Playbook revolve around?
- How many phases are there?

Module 3

Cyber Risk Assessor (CRA)



CRA Roles and Responsibilities

- The Cyber Risk Assessor (CRA) is responsible for providing the Authorizing Official (AO) with an independent "Cyber Risk Analysis" and acceptable "Risk of Use" for the System or Capability throughout the entire Agile Authorization process while focusing on criteria, observables, and overall behaviors.
- **Responsibilities**
  - Develop, review, and approve a plan to assess the security requirements.
  - Assess the requirements employed within or inherited by the information system using procedures specified in the security assessment plan, and
  - Provide specific recommendations on how to correct weaknesses or deficiencies and reduce or eliminate identified vulnerabilities.
  - Conduct initial remediation actions on the findings and recommendations of the security assessment report and reassess remediated mitigations, as appropriate.
  - Assess a selected subset of the technical, management, and operational security controls employed within and inherited by the information system in accordance with the organization-defined monitoring strategy.
  - Prepare the final authorization package, create, and submit the Risk Assessment Report, Risk Recommendation Letter and will submit to and obtain the authorizing official's signature on the authorization decision document(s), and transmit the authorization package to appropriate officials.
  - Can be empowered by authorizing officials to make certain decisions about the planning and resourcing of the security authorization process, approval of the security plan, approval and monitoring the implementation of plans of action and milestones, and the assessment and/or determination of risk.

CRA Objectives, Onboarding and Playbook

- **Objectives**
  - Overall CRA goals and basic introduction to the Fast-Track Agile Authorization process (Key steps/documents).
- **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.
- **Playbook**
  - Outlines the Agile Authorization Process, Objectives , step by step approach along with the templates used when interacting with the AO for authorization decisions.

Objectives - Simplified Authorizations

- **Objective 1:** Systems/Systems Security Engineering, Evidentiary Data & Analysis
  - Architecture(s)
  - System Boundary(s)
  - Functional Requirements
  - Decomposition (Breakdown)
  - Data Flows
  - Technologies
  - Previous assessments?
  - Test results (Red/Blue/Etc.)
    - **Output - Standard Acquisition Systems Engineering Data**

Objective 2: Collaboration with AO

- Discuss risk assessment and way ahead
- Previous assessments, analysis results
- Operational Use
- Perspective
- **Output - Scope the assessment criteria and outcomes**

Objective 3: Execute Risk Assessment

- Tool Agnostic – Focus on
- Evidentiary Data and Analysis
- Clinically define Risk of Use Posture
- Outline Mitigations for Risks
- **Output - Provide Determination Briefing to AO**

CRA Onboarding

- **Appointment Letter** - Ensure you have one and anticipate a one on one with the AO to understand your expectations.
- **Key Websites** – Be familiar with these. They provide you the tools necessary to be successful.
- **AO Support:**
  - You are the POC between the program and the AO (Program contact information, ITCSC, Assessment activities, Reports, CRA Recommendations, Draft AO Letter, ConMon activities, AO Briefings, AO Tag Up Briefs, Ad hoc meetings, etc.)
- **Focus on the Objectives and the Risks**
  - This is not a checkbox effort
  - What is the Risk of Use? This is what the AO wants to know…
- **Learn the A&A Lifecycle –** Understand what's required at each step of the process – keep it simple.
- **Key Documents –** Work with your programs to obtain the details necessary to complete.

  - ITCSC
  - AO Determination Brief
  - CRA Recommendation Letter
  - DRAFT Authorization Letter
  - Risk Assessment Report

CRA Playbook

1. **Categorize System** - Categorize the information system and document the results in the AO Determination Brief

2. **Select Security Requirements** - Identify the security requirements that are provided by the organization as common requirements for organizational IS and document the requirements in the AO Determination Brief and SSP.

3. **Implement Security Requirements** - Implement the security requirements specified in the SSP and AO Determination Brief

4. **Assess Security Requirements** - Determine Assessment Criteria, develop, review, and approve a plan to assess the security requirements

5. **Authorize System** - Prepare the Plan of Action and Milestones (POA&M) based on the findings and recommendations of the SAR, including any remediation actions taken.

6. **Monitor Security Requirements** - Determine the security impact of proposed or actual changes to the IS and its environment of operation.

7. **Decommission/Disposition/Sunset** - Implement an IS Decommissioning Strategy, when needed, which executes required actions when a system is removed from service.

Questions

- What is the CRA's Role?
- What is the CRA's 3 objectives?
- Does the CRA require an appointment letter?
- Who signs that letter if one is required?
- What types of activities are the CRA's responsible for?
- Has the AO provided the CRA with tools to meet their objectives?
- What are the key tools/artifacts that are communicated to the AO?
- If an authorization is provided, are there any initiatives beyond that?

Module 4

Body of Evidence, Artifacts - Information Tools

Artifacts -Information Tools

1. **AO Determination Briefing** - The objective of the brief is to assist program personnel in understanding what the AO is expecting to make an informed risk determination.
2. **AO Determination Briefing Guide** - The guide provides additional notes, references and details about each slide when completing the AO Decision Brief.
3. **AO Level 1 Playbook** - High-level introduction outlining the Agile Authorization Process, Objectives, and Criteria 4-phase process along with the templates used when interacting with the authorizing official for authorization decisions.
4. **AO Objectives** - Articulates the AO goals, enablers for success and collaboration needed for execution - (part of the AO Playbook Level 1)
5. **CRA Objectives** - Overall CRA goals and basic introduction to the Fast-Track High Level Agile Authorization process (Key steps/documents).
6. **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.

Artifacts - Information Tools Continued

10. **CRA Risk Recommendation Letter** - Defines the results from the formal Security Assessment, outlining all vulnerability and weaknesses found and defining recommended conditions for the program to follow in correcting each found item.
11. **DevSecOps (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.
12. **Draft AO Authorization Letter -** A formal written statement by the Authorizing Official regarding the risk associated with operating the information system (IS) and expressed as an authorization to operate (ATO), interim authorization to test (IATT), or denial of ATO (DATO) etc.
13. **IT Categorization and Selection Checklist (ITCSC)** - Process of determining the security category for information or an information system. This checklist helps in determines impact values: (i) for the information type(s) processed, stored, transmitted, or protected by the information system; and (ii) for the information system and identify overlays that apply to the information system and its operating environment to account for additional factors (beyond impact) that influence the selection of security requirements.
14. **No Security Impact** – CRA/ISSM written recommendation that there are no security impacts on the **No Security Impact (NSI) Template** organizational operations, 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.

Agile Authorizations: Authorization Package and BOE

- **Authorization Package**
  - AO Determination Brief + RAR
  - AO Authorization Memo
  - CRA Risk Recommendation Letter
  - ITCSC

Authorization Package

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.

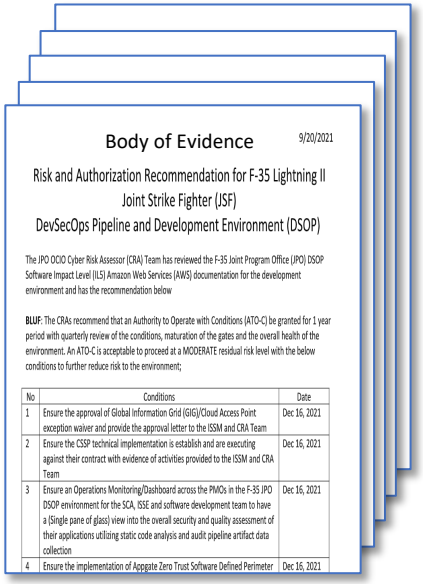
3. (U) This determination is based on the assessment of the security posture, identified risks, system specific requirements, proposed and agreed to mitigations, and all supporting documentation evaluated in accordance with AF and DOD guidance. Key documents from the Body of Evidence (BOE) reviewed are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



Body of Evidence 9/20/2021

Risk and Authorization Recommendation for F-35 Lightning II Joint Strike Fighter (JSF) DevSecOps Pipeline and Development Environment (DSOP)

The JPO OCIO Cyber Risk Assessor (CRA) Team has reviewed the F-35 Joint Program Office (JPO) DSOP Software Impact Level (IL5) Amazon Web Services (AWS) documentation for the development environment and has the recommendation below

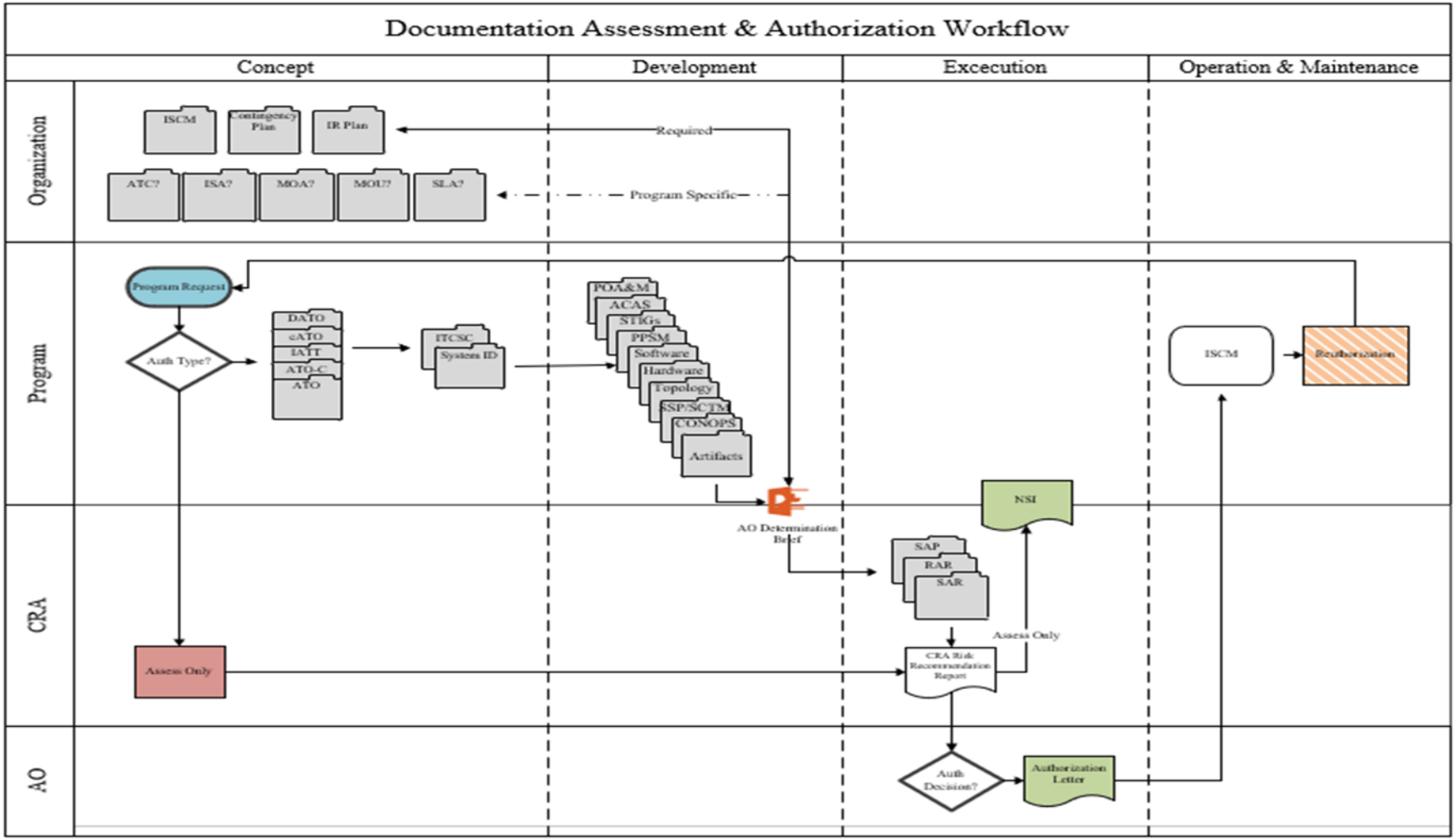
BLUF: The CRAs recommend that an Authority to Operate with Conditions (ATO-C) be granted for 1 year period with quarterly review of the conditions, maturation of the gates and the overall health of the environment. An ATO-C is acceptable to proceed at a MODERATE residual risk level with the below conditions to further reduce risk to the environment;

No	Conditions	Date
1	Ensure the approval of Global Information Grid (GIG)/Cloud Access Point exception waiver and provide the approval letter to the ISSM and CRA Team	Dec 16, 2021
2	Ensure the CSSP technical implementation is establish and are executing against their contract with evidence of activities provided to the ISSM and CRA Team	Dec 16, 2021
3	Ensure an Operations Monitoring/Dashboard across the PMOs in the F-35 JPO DSOP environment for the SCA, ISSE and software development team to have a (Single pane of glass) view into the overall security and quality assessment of their applications utilizing static code analysis and audit pipeline artifact data collection	Dec 16, 2021
4	Ensure the implementation of Appgate Zero Trust Software Defined Perimeter	Dec 16, 2021

- **Body of Evidence, but not limited to**
  - SSP
  - CONOPs
  - POA&M
  - SCTM
  - STIG's
  - ACAS Scans
  - SAP & SAR
  - ConMon Plan
  - Incident Response Plan
  - Contingency Plan

Standardization is flexible for authorization packages: There is no one-size-fits-all approach.

Documentation A&A Life Cycle



Questions

- Should the CRA be very clear upfront in terms of what they are asking the program to provide?
- What is included in the Body Of Evidence to the AO?
- What other artifacts must be completed, but not necessarily provided as part of the Authorization Package?
- In reference to the A&A lifecycle, what is the organization responsible?
- What is the program responsible for?
- Who updates the system artifacts?

Module 5

CRA Assessments

Assess Only

- All IT Services and Products have cybersecurity considerations even though they might not be authorized for operation by implementing the full process. However, cybersecurity requirements must still be identified, tailored appropriately, and assessed or evaluated before operational use, whether they are included in a system's authorization boundary or not.

- All assessments must provide the due diligence review and assessment commensurate with the type of product, or service and the risks associated.

- The Assess Only construct identifies two assessment approaches:

  - 1) the Assess, Approve for Use, and Inherit which addresses IT products and services that are assessed, but "**do not become**" part of an authorized system's authorization boundary, and

  - 2) the Assess and Incorporate approach which addresses IT products or services that "**will become**" part of another authorized system's authorization boundary.

Assessment Tools

1. **Security Assessment Plan** - The security assessment plan "***identifies objectives for the security assessment"***, a roadmap describing how to conduct the assessment, and points to the detailed assessment procedures.

2. **Security Assessment Report** - The SAR "***documents the CRA's findings"*** with assigned requirements based on actual assessment results. It addresses findings in a non-mitigated status, including existing and planned mitigations.

3. **Risk Analysis Report** - This report is focused on "***risk assessment of non-mitigated risks and addresses vulnerabilities and weaknesses displayed in the SAR after the assessment"*** has been completed by the CRA. All non-mitigated risks must be subjected to a risk assessment that considers multiple factors in assigning a residual risk level to each non-mitigated requirement. The individual risk levels are then used to inform the CRA's recommendation (i.e., SAR executive summary) to the AO on acceptance of the cybersecurity risk of operating the system.

Security Assessment Plan

- The CRA develops the security assessment plan, and the AO or AODR reviews and approves the plan.
    - Establish the appropriate expectations for the assessment and to bound the level of effort.
- Identify the objectives, a roadmap describing how the assessment will be conducted.
    - Simple a high-level plan for completing the task of assessing the requirements for the specific system(s).
    - Consideration should be given to starting assessments early, before development and integration of all components is completed; and to leverage the results of testing done by developers and integrators. This allows for early identification and correction of deficiencies and completion of assessments in a timely manner.
- Ensure the plan is consistent with the security objectives of your organization; employ state-of-the-practice tools, techniques, procedures, and automation to support the concept of information security monitoring and near real-time risk management; and is cost-effective regarding the resources allocated for the assessment.
    - Ensuring that appropriate policies covering assessments are in place and understood by all affected organizational elements;
    - Ensuring that all steps in the process prior to the assessment step, have been successfully completed and received appropriate management oversight;
    - Ensuring that requirements identified as common controls (and the common portion of hybrid controls) have been assigned to appropriate organizational entities (i.e., common control providers) for development and implementation
    - Establish the objective and scope of the assessment (i.e., the purpose of the assessment and what is being assessed)

Security Assessment Plan – Talking Points

- What is the AO looking for? Defer to the Determination Brief.
  - Hygiene Risk Areas?
- Review and "understand" your evidence
- From the requirements (controls) break them down to control types.
  - Technical, Operational and Management – know these!
- Determine which requirements need to be assessed during the actual assessment and what you can determine by the provided evidence?
  - Example – Technical requirements will be assessed via STIGs/scans.
  - O&M – Most of these requirements will be achieved in the evidence/documentation.
  - Upfront - Do we know what requirements have not been met?

Security Assessment Report

- The results of the security control assessment, including recommendations for correcting any weaknesses or deficiencies in the controls, are documented in the security assessment report (SAR).

- The SAR includes information from the assessor necessary to determine the effectiveness of the security controls employed within or inherited by the information system based upon the assessor's findings. The SAR is the primary document used by an authorizing official to determine risk to organizational operations and assets, individuals, other organizations, and the Nation.

- The SAR documents the security control assessor (CRA's) findings of compliance with assigned security controls based on actual assessment results. It addresses security controls in a non-compliant (NC) status, including existing and planned mitigations. If a compelling mission or business need requires the rapid introduction of a new IS or PIT system, assessment activity and a SAR are still needed.

Cyber Hygiene Areas
AO Emphasis (Superset)

*Red font indicates specific JSIG, Non-Tailorable controls

#	Cyber Hygiene Area (associated controls)	Version 1.0		Version 2.0
		Weapons	SAP (JSIG)	Weapons, SAP, Cloud, DSOP
1.0	Account Management (Aligns to ORTB: AC-2)		X	X
2.0	Administrative Privileged Accounts (Aligns to ORTB: AC-6)	X	X	X
3.0	Audit Review, Analysis, and Reporting (Aligns to ORTB: AU-6)		X	X
4.0	Boundary Protection (Aligns to ORTB: SC-7)		X	X
5.0	Continuous Monitoring (Aligns to ORTB: CA-7)		X	X
6.0	Data Integrity (Aligns to ORTB: SI-7)	X		X
7.0	External Connections (Aligns to ORTB: CA-3)		X	X
8.0	External Media (Aligns to ORTB: AC-4, MP-7)	X		X
9.0	Information Flow Enforcement (Aligns to ORTB: AC-4)		X	X
10.0	Least Privilege (Aligns to ORTB: AC-6)		X	X
11.0	Operational Change Management (Aligns to ORTB: CM-8, CM-8(3))			X
12.0	Proposed Equipment (Aligns to ORTB: SA-22 – applies to C.I.A. impact High on non-SAP systems, CM-3)	X	X	X
13.0	Protection of Information at Rest (Aligns to ORTB: SC-28, SC-28(1))		X	X
14.0	Secure Baseline Configuration (Aligns to ORTB: CM-2, CM-6)		X	X
15.0	Security Categorization (Aligns to ORTB: RA-2)		X	X
16.0	Separation of Duties (Aligns to ORTB: AC-5)		X	X
17.0	Vulnerability / Anti-Virus Scanning (Aligns to ORTB: RA-5)	X	X	X

Cyber Hygiene Areas
AO Emphasis (Superset)

*Red font indicates specific JSIG, Non-Tailorable controls

Account Management (Aligns to ORTB: AC-2)
- Monitor and Enforce user and group account creation/deletion

Administrative Privileged Accounts (Aligns to ORTB: AC-6)
- Privileged user/service accounts are only authorized to perform security relevant functions. Review and approve annually.

Audit Review, Analysis, and Reporting (Aligns to ORTB: AU-6)
- Review and analyze Information System (IS) audit logs for indications of inappropriate or unusual activity and reports findings to designated personnel IAW IRP

Boundary Protection (Aligns to ORTB: SC-7)
- Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system

Continuous Monitoring (Aligns to ORTB: CA-7)
- System level monitoring metrics, including control monitoring frequencies, are defined by the organization and approved by the AO

Data Integrity (Aligns to ORTB: SI-7)
- Employ automated tools to report system (hw/sw/fw) and information (data) integrity violations. Ensure automatic integrity validation of all electronically transmitted software and data

External Connections (Aligns to ORTB: CA-3)
- Agreement/authorization used to approve external connections and manage the exchange of information should be defined (ATC, ISA, CSA, ICD, etc.) and reviewed annually

External Media (Aligns to ORTB: AC-4, MP-7)
- If authorized, place configuration control process on all external media including auditing. Institute external media whitelisting. Implement processes to monitor logs and audit usages.

Information Flow Enforcement (Aligns to ORTB: AC-4)
- The information system enforces approved connections for controlling the flow of information within the system and between interconnected systems

Least Privilege (Aligns to ORTB: AC-6)
- Reviews, at least annually, the privileges assigned to privileged user accounts including Designated Transfer Agent and Trusted Cloud Credential Manager roles

Operational Change Management (Aligns to ORTB: CM-8, CM-8(3), SI-7)
- Automated mechanisms shall be used to detect the presence of unauthorized hardware/software/firmware within the system. One or more of the following action shall be taken upon discovery of unauthorized components: disable network access by unauthorized components; isolate unauthorized components; notify designated personnel identified in IRP

Proposed Equipment (Aligns to ORTB: SA-22 – applies to C.I.A. impact High on non-SAP systems, CM-3)
- Lock down all mission support systems and migrate off unsupported operating systems. Review support agreements (hw/sw/fw) annually

Protection of Information at Rest (Aligns to ORTB: SC-28, SC-28(1))
- Encryption is implemented to complement protection of information at rest, using approved cryptographic methods for data encryption

Secure Baseline Configuration (Aligns to ORTB: CM-2, CM-6)
- This Information System's secure configuration includes DoD Security Technical Implementation Guides or industry best practices and verified conformance prior to introduction into production or operational environments

Security Categorization (Aligns to ORTB: RA-2)
- Enforce proper security categorization and review annually

Separation of Duties (Aligns to ORTB: AC-5)
- Separates defined duties of individuals and documents separation of duties of individuals

Vulnerability / Anti-Virus Scanning (Aligns to ORTB: RA-5)
- Conduct routine anti-virus scans on traditional IT systems and hosted applications. Institute continuous monitoring protection on all IT systems to include maintenance and testing support systems

Body Of Evidence

- AO Determination Briefing;
- ATO Package, including CRA Risk Assessment;
- Signed Information Technology Security Categorization and Selection Checklist (ITSC);
- System Security Plan
- Topology*
- Hardware List*
- Software List*
- Security Technical Implementation Guide (STIG) applicability list
- Ports, Protocols, and Service Matrix and registration number
- Vulnerability scans (if applicable, analyzed and sated within 60 days of submission)
- STIG Compliance scans (if applicable, analyzed and dated within 60 days of submission)

Note: BOE Items Required to be in CORE folder prior to Authorization approval

*** Items Marked can be included as part of the System Security Plan Or can be referenced in the AO Determination Briefing**

Connection Package Required Documentation

- Interconnection Security Agreement (ISA) signed by AO
- Authorization to Operate - Signed by AO
- Existing ISAs/ATCs and ATOs for other external connections
- RAW Scan files (Nessus, XCCDF, etc.)
- Evidence that all scans were credentialed
- Topology includes device function, OS, IP address, make/model
- POA&M must include all CAT I and Critical findings from scans on all devices

Note: BOE Items Required to be in CORE folder prior to Authorization approval

Risk Assessment Report – Talking Points

- **Purpose for Risk Assessment** -determine risk at various levels, categorization, tailor requirements, assess non-mitigated requirements etc.
- **POC's** – Name, phone number, email etc.
- **Scope** - The scope of the risk assessment can be at any of the three tiers in the risk management hierarchy (i.e., organization, mission/business process, or system), or the scope can be limited to certain portions of the system
- **Assessment Approach** - Identify the type of risk assessment methodology used (qualitative, semi-quantitative, or quantitative)
- **Analysis Approach** - Threat-based, Vulnerability Based, or Asset Impact Based
- **Organizations Risk Tolerance** - The level of risk an entity is willing to assume in order to achieve a potential desired result; Identify any organization risk tolerance levels set at Tier 1, Tier 2, and Tier 3
- **Threat Sources** - Identifies threat sources that could initiate the threat event
- **Threat Source Capability** - Indicates the adversarial threat source's capability to initiate a threat event
- **Threat Source Intent** - Indicates the adversarial threat source's intent to initiate a threat event
- **Threat Source Targeting** - Indicates if the adversarial threat source has historically targeted or is actively targeting the system
- **Threat Event** - Identifies the potential threat event
- **Vulnerability or Predisposing Condition** - Identifies vulnerabilities which could be exploited by threat sources and the predisposing conditions which could increase the likelihood of undesirable consequences and/or adverse impacts
- **Vulnerability Severity or Pervasiveness of Predisposing Condition** - Identifies the severity of vulnerabilities or the pervasiveness of the predisposing conditions as low, moderate or high.
- **Likelihood of Threat Event Initiation/Occurrence** - Indicates the likelihood the threat event will be initiated or occur, taking into consideration the adversarial threat source's capability, intent, and targeting; non-adversarial threat source's historical evidence and empirical data; timeframe and frequency of event; state of the organization
- **Likelihood of Threat Event Success** - Determine the likelihood the threat event, once it is initiated or occurs, will result in an adverse impact, regardless of the magnitude of harm (i.e., impact)
- **Overall Likelihood** - Indicates the likelihood the threat event will be initiated or occur and result in adverse impact (i.e., combination of likelihood of threat event initiation/occurrence and likelihood the initiated event succeeds)

Risk Analysis Report

Risk # R1	Area of Concern (xxx)	Mechanisms (xxx)	Initial Risk Level (xxx)
Threat: <Describe the specific threat/threats that can potentially exploit this vulnerability.>			
Vulnerability: <Describe the vulnerability.>			
Likelihood: <What is the likelihood? Describe the likelihood of the vulnerability being exploited. Use means and opportunity.>			
Impact: <What is the impact? Describe the impact of the vulnerability being exploited. Use criticality and impact.>			
Mitigations In Place: <Describe the mitigations already in place.>			
ADDITIONAL MEASURES APPLIED TO THE SYSTEM			
Countermeasures Added: <Describe additional mitigations to lower the likelihood or impact of this vulnerability being exploited.>			
Residual Risk: <If mitigations in place and or added countermeasures lowered the likelihood or impact, then the residual risk level could be lowered.>			***Residual Risk*** (xxx)
Additional Countermeasures Suggested: <What further actions will be taken to reduce likelihood/impact in the future?>			

Risk Scale Summary

R1 – Initial Risk Level
R1* – Residual Risk Level

LEVEL OF IMPACT

LIKELIHOOD	VERY LOW	LOW	MODERATE	HIGH	VERY HIGH
VERY HIGH	Very Low	Low	Moderate	High	Very High
HIGH	Very Low	Low	R2* Moderate	R2 High	Very High
MODERATE	Very Low	Low	R1 Moderate	R3 Moderate	High
LOW	Very Low	R1* Low	R3* Low	Low	Moderate
VERY LOW	Very Low	Very Low	Low	Low	Low

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

POA&M

- The purpose of a Plan of action and Milestones (POA&M) is to assist agencies in identifying, assessing, prioritizing, and monitoring security deficiencies found in programs and systems, and to document progress in correcting those deficiencies. OMB requires agencies to prepare POA&Ms for all programs and systems where security deficiencies have been found.

- The POA&M is designed to be a management tool to assist agencies in closing their security performance gaps, assist inspectors general (IGs) in their evaluation work of agency security performance, and assist OMB with oversight responsibilities.

- POA&Ms are permanent records. Once posted, entries are updated, but not removed even after correction or mitigation actions are completed. Inherited deficiencies are also reflected on the POA&Ms.

- DoD is responsible for maintaining the confidentiality of POA&Ms because they may contain pre-decisional budget or other sensitive information.

Questions

- What are the 2 different types of assessment approaches in an assess only effort?
- What is the Security Assessment Plan for?
- What is the Security Assessment Report for?
- What is the Risk Assessment Report For?
- Should the CRA provide an In/Out brief to every assessment?
- Are hygiene areas important?
- Can the AO change the risk level?
- Is there an adjudication process?

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

Module 6

Continuous Execution

Continuous Monitoring

- **System and Environmental Changes**
  - Program should conduct a security impact analysis
    - Do the proposed or actual changes to the system or its environment of operation affect the security state of the system?
    - No security-related changes to the system or its environment of operation should be implemented without first consulting with appropriate organizational officials/entities (e.g., configuration control board, SISO, CRA).
    - The AO/AODR uses the revised and updated artifacts to determine if a formal reauthorization action is necessary.
    - Most routine changes to a system or its environment of operation can be handled by the organization's ISCM program, thus supporting near real-time risk management; however, for the most critical controls, automated tools (e.g., dashboards) may be required to provide timely notifications and allow for quick responses.
- **Ongoing Remediation Actions**
  - This task is focused on conducting remediation actions based on the results of ISCM activities, assessment of risk, and outstanding items in the POA&M.
- **Key Updates**
  - This task includes updating the SP, RAR, SAR, and POA&M based on the results of the ISCM process.
  - The ISSM/ISSO must assist the CRA in updating and maintaining the RAR and SAR based on the results of ISCM.
- **Security Status Reporting**
  - This task is focused on reporting the security status of the system (including the effectiveness of security requirements employed within and inherited by the system) to the AO and other appropriate organizational officials on a continuous basis in accordance with the ISCM strategy.
- **Ongoing Risk Determination and Acceptance**
  - This task includes the AO reviewing the reported security status of the system (including the effectiveness of security requirements employed within and inherited by the system) on a continuous basis in accordance with the ISCM strategy to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation remains acceptable. The AO responds accordingly to the changed security status, which may include changing the authorization decision from an ATO to an ATO with conditions, or to a DATO.
- **System Removal and Disposal (Decommissioning)**
  - This task is focused on implementing a system decommissioning strategy, when needed, and involves executing required actions when a system is removed from service.
  - The ISO is responsible for implementing a system decommissioning strategy, when one is needed.

Conditions and Residual Risk

- **Source documents**
  - CRA Risk Recommendation Letter
  - AO Authorization Letter
  - Risk Assessment/Analysis Report
  - Plan of Action and Milestones
  - DISA STIGs/Scans
  - SCAP Compliance
- **Level of Impact** - Determine the level of impact associated with the undesirable consequences of the threat event (i.e., potential harm to organizational operations, organizational assets, individuals, other organizations, or the Nation) of the threat event.
- **Residual Risk Level** - For individual entries in the RAR, indicates the residual risk level expected after mitigations are implemented (as described in the POA&M). Identifies the risk level as one of the following, low, moderate or high).
- **Number of requirements with Risks identified** - Indicates the number of requirements identified for each level of risk (i.e., low, moderate or high)
- **Overall Risk Posture** - Describe the overall level of risk (e.g., low, moderate or high,) to the system, considering all individual risks, mitigating factors, environment, architecture, system's security categorization, historical evidence, etc.

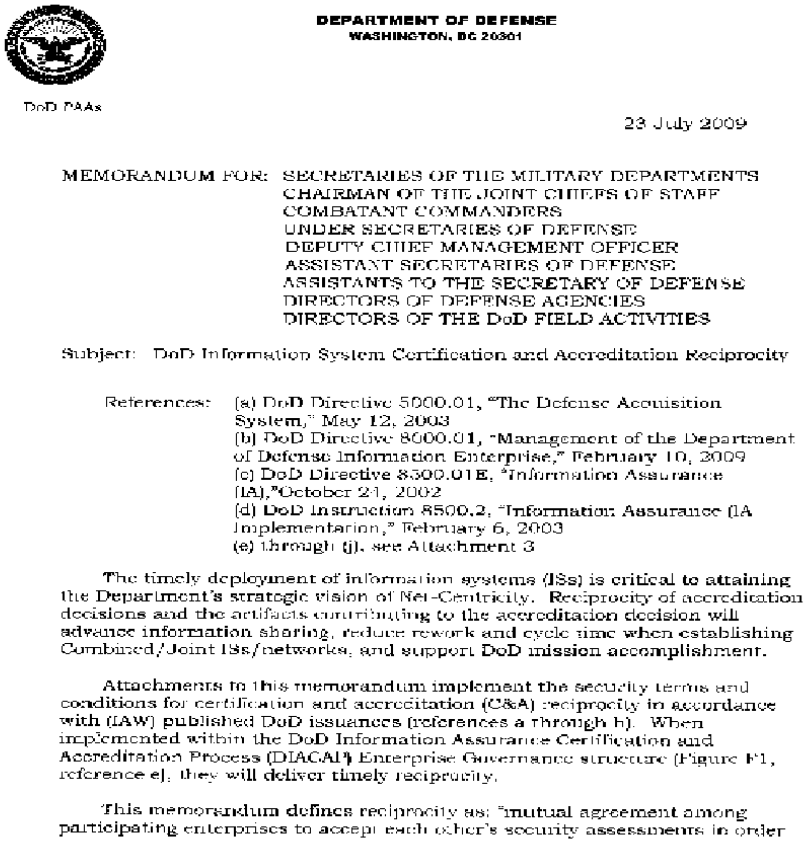
No Security Impact

- **Minor and or No Security impact -** hardware and software changes to information systems may require AO authorization. These upgrades require an administrative update to the SSP. Examples of non-security-relevant changes include:
  - No-security impact software version updates and/or upgrades.
  - Addition of identical workstation type with approved image to an authorized system.
  - Replacement of failed servers/system components with identical spares.
  - Replacement of hard drives/tape back-up.

- **Security Impacting Changes -** any hardware or software that is "security enforcing," "security supporting," or "security non-interfering" which can affect an IS's configuration, functionality, or users' privileges, and has the potential to change the risk imposed on the IS.
  - Changes that modify the security support structure.
  - Operating system changes (e.g., Windows 7 to Windows 10).
  - Security Relevant software version upgrades (e.g., Update to Microsoft Office beyond AFT tool capabilities, firmware update for security appliances).
  - Addition of security relevant software not previously approved for the systems.
  - Addition of new server function.
  - New hardware models
  - Modification to system ports, protocols and services (PPS).
  - Major vulnerabilities discovered after assessment and/or authorization.
  - Changes to the confidentiality, integrity, or availability requirements (e.g., changing from a moderate impact level to high impact level).
  - Changes in system encryption methods.
  - Changes to interconnections.
  - Changes to operating environment (e.g., external information system introduces media capability; introduction of Voice over Internet Protocol (IP) (VoIP) (classified or unclassified); foreign nationals move in next door; system is relocated).
  - Significant increased threat increasing the organization/site's residual risk.

Reciprocity

- **Reuse Information System Resources and Decrease Work Effort**
- **Interoperability**
- **Level of trust based off transparency**
- **Uniform processes**
- **Cost savings**
- **Improved Scheduling**
- **Evidence to current and future stakeholders**



DEPARTMENT OF DEFENSE
WASHINGTON, DC 20301

DoD CAAs

23 July 2009

MEMORANDUM FOR: SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
COMBATANT COMMANDERS
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
ASSISTANT SECRETARIES OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTORS OF DEFENSE AGENCIES
DIRECTORS OF THE DoD FIELD ACTIVITIES

Subject: DoD Information System Certification and Accreditation Reciprocity

References: (a) DoD Directive 5000.01, "The Defense Acquisition System," May 12, 2003
(b) DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise," February 10, 2009
(c) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
(d) DoD Instruction 8500.2, "Information Assurance (IA Implementation," February 6, 2003
(e) through (j), see Attachment 3

The timely deployment of information systems (ISs) is critical to attaining the Department's strategic vision of Net-Centricity. Reciprocity of accreditation decisions and the artifacts contributing to the accreditation decision will advance information sharing, reduce rework and cycle time when establishing Combined/Joint ISs/networks, and support DoD mission accomplishment.

Attachments to this memorandum implement the security terms and conditions for certification and accreditation (C&A) reciprocity in accordance with (IAW) published DoD issuances (references a through h). When implemented within the DoD Information Assurance Certification and Accreditation Process (DIACAP) Enterprise Governance structure (Figure F1, reference e), they will deliver timely reciprocity.

This memorandum defines reciprocity as: "mutual agreement among participating enterprises to accept each other's security assessments in order

Reciprocity Agreements and Conditions

- **Current Agreements:**
  - Stakeholders?
  - Obtain and understand what is currently in place?
- **Current Conditions:**
  - What has or has not been done and why?
  - How does that impact your environment/goals?

Reciprocity - Joint Responsibilities

- **Prior to entering into an agreement, or deploying a type-authorized system, receiving and originating organizations need to complete several tasks. These tasks may include:**
  - Identify who is responsible for providing the resources (e.g., funding, hardware, software, and personnel) required managing and operating the system.
  - Verify compliance and maintenance of the type authorization by the originating organization.
  - Ensure the receiving organization implements the appropriate installation security requirements required by the authorization package and applies mitigation strategies as directed by the originating organization's Plan of Action & Milestones (POA&M).
  - Ensure the type authorization and/or interconnected systems are not adversely affected by new (or aggregated) vulnerabilities.
  - Verify and maintain the correct configuration.
  - Ensure all stakeholders have access to the complete security authorization package, to include configuration specifications.
  - Formally document all tasks that must be completed and the associated responsible organization, as the result of agreement between the originating and receiving organizations.

Reciprocity - Responsibilities of Originating Organization

- Provide the security authorization package and deployment instructions (or access to it) including a current POA&M, to receiving organizations.
- Communicate all changes to the system during its lifecycle (i.e., different version) to receiving organizations.
- Notify receiving organizations of any new findings (e.g., new threats, discovered vulnerabilities, etc.) throughout the authorization life cycle.
- Gather requirements from potential leveraging organizations before developing the system, to ensure the widest use of a standardized configuration and avoid one-off modifications driving separate authorizations.
- Provide a point of contact (POC) to receiving organizations requesting information
- Notify receiving organizations at least six months prior to any reauthorization events to ensure consideration of any input from receiving organizations.
- Notify receiving organizations of any plans that may affect their use of the system (e.g., decommissioning, version changes, etc.).
- Identify factors or conditions justifying termination of the MOU/MOA
- Communicate and provide patches and updates in accordance with DoD and USCBYERCOM requirements and timelines.
- Maintain deployment locations of the system within originating organizational authorization tracking tool.
- Ensure assignment of a USCYBERCOM accredited Cybersecurity Service Provider (CSSP) to maintain continuous monitoring, patch management, Information Assurance
- Vulnerability Management (IAVM) Program, operational orders, POA&M, annual reviews, and/or quarterly/monthly reviews of authorized systems.

Reciprocity - Responsibilities of Receiving Organization

- Request Security Authorization Package and deployment instructions (or access to it), including a current POA&M, from the Originating Organization.
- Accept the originating organization AO's authorization decision.
- Deploy the system using configuration requirements in the security authorization package and deployment instructions.
- Provide all inherited security controls, mitigations, or support functions required by the type authorization.
- Obtain any necessary authorization to connect and operate the system within the organization's network.
- Provide a single POC to originating organizations providing information.
- Update necessary authorization tracking tools within the organization.
- Implement required patches and changes in accordance with Project Management (PM) guidance.
- Notify originating organizations of any new findings (e.g., new threats, discovered vulnerabilities) throughout the authorization life cycle.
- Implement mitigations in accordance with the originating Information Technology Security POA&M.

Reciprocity – Change Management

- All organizations must identify technical POCs as part of their MOU, MOA and/or SLA to support the management and operation of the type-authorized system. Organizations must communicate to the PM and/or original AO any event that may affect the security posture of the type-authorized system or the installed environment. Agreements must include processes, timing, and notification requirements.
- **Examples of events**:
  - Deploy the system using configuration requirements in the security authorization package and deployment instructions.
  - Provide all inherited security controls, mitigations, or support functions required by the type authorization.
  - Obtain any necessary authorization to connect and operate the system within the organization's network.
  - Provide a single POC to originating organizations providing information.
  - Update necessary authorization tracking tools within the organization.
  - Implement required patches and changes in accordance with Project Management (PM) guidance.
  - Notify originating organizations of any new findings (e.g., new threats, discovered vulnerabilities) throughout the authorization life cycle.
  - Implement mitigations in accordance with the originating Information Technology Security POA&M.

eMASS Guidance

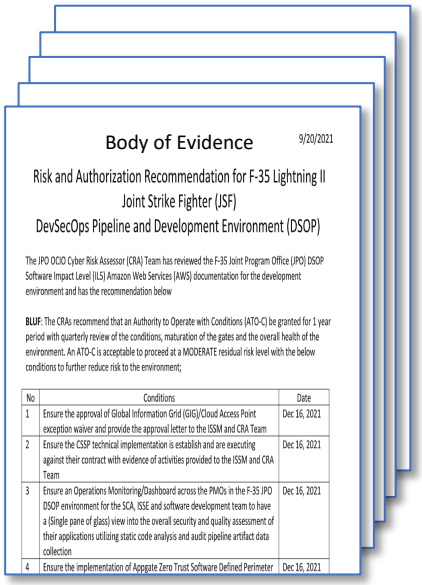
- **Authorizing Official (AO)**
  - Renders authorization determination, balancing mission needs and security concerns in their boundary.
  - Authorization Determination is in eMASS
    - ATO Package meets requirement
    - Can be uploaded to either eMass, Xacta, or any other tool – authorization is agnostic to the tracking tool

- **Cybersecurity Risk Assessors (CRA)s {Per specific boundary requirements}**
  - Assess and identify Risk of use based on program provided evidentiary data and analysis;
  - Provide AO an independent (of the program chain of command) risk recommendation including:
    - Draft Authorization recommendation memo;
    - CRA Recommendation Memo, including attachments for:
      - Risk analysis report;
      - ITSC (Jointly developed with the Program ISSM);
      - AO Determination Briefing
      - Other as applicable (e.g., DevSecOps CONOPS, etc.)
  - Validate controls in eMASS to support reciprocity and assist with uploading authorization package as needed

- **Program Manager (PM) Responsibility**
  - Ensures Cybersecurity and Resilience requirements, attributes, and design consideration are designed into newly acquired systems and modified systems
  - 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 (ITSC)
    - Cybersecurity Strategy
    - Authorization Memo

Authorization Package Available in eMASS

- **Will document the key items needed for reciprocity:**
  - Authorization Memo.
  - Attachment 1: Conditions.
  - Attachment 2: Body of Evidence.
  - Attachment 3: Authorization Package.



Body of Evidence 9/20/2021

Risk and Authorization Recommendation for F-35 Lightning II Joint Strike Fighter (JSF) DevSecOps Pipeline and Development Environment (DSOP)

The JPO OCIO Cyber Risk Assessor (CRA) Team has reviewed the F-35 Joint Program Office (JPO) DSOP Software Impact Level (IL5) Amazon Web Services (AWS) documentation for the development environment and has the recommendation below

BLUF: The CRAs recommend that an Authority to Operate with Conditions (ATO-C) be granted for 1 year period with quarterly review of the conditions, maturation of the gates and the overall health of the environment. An ATO-C is acceptable to proceed at a MODERATE residual risk level with the below conditions to further reduce risk to the environment;

No	Conditions	Date
1	Ensure the approval of Global Information Grid (GIG)/Cloud Access Point exception waiver and provide the approval letter to the ISSM and CRA Team	Dec 16, 2021
2	Ensure the CSSP technical implementation is establish and are executing against their contract with evidence of activities provided to the ISSM and CRA Team	Dec 16, 2021
3	Ensure an Operations Monitoring/Dashboard across the PMOs in the F-35 JPO DSOP environment for the SCA, ISSE and software development team to have a (Single pane of glass) view into the overall security and quality assessment of their applications utilizing static code analysis and audit pipeline artifact data collection	Dec 16, 2021
4	Ensure the implementation of Appgate Zero Trust Software Defined Perimeter	Dec 16, 2021

Authorization Package

|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

- **Attachment 1: Conditions**
  - Documents any conditions on the ATO.
  - Security is a journey, never a destination.
- **Attachment 2: Body of Evidence**
  - Key artifacts reviewed that support the recommendation (SSP, CONOPs, H/W, S/W, Assessment Reports etc.).
  - Informs other AOs and consumers to increase reciprocity.
- **Attachment 3: Authorization Package**
  - Key artifacts generated that support the authorization package (AO Determination Briefing, CRA Risk Recommendation Letter, ITCSC and POA&M).
  - Can be a Classified appendix.

- *Provided to the requesting consumer as a contract*
- *Documented in enterprise tools (e.g., eMass, XACTA….)*

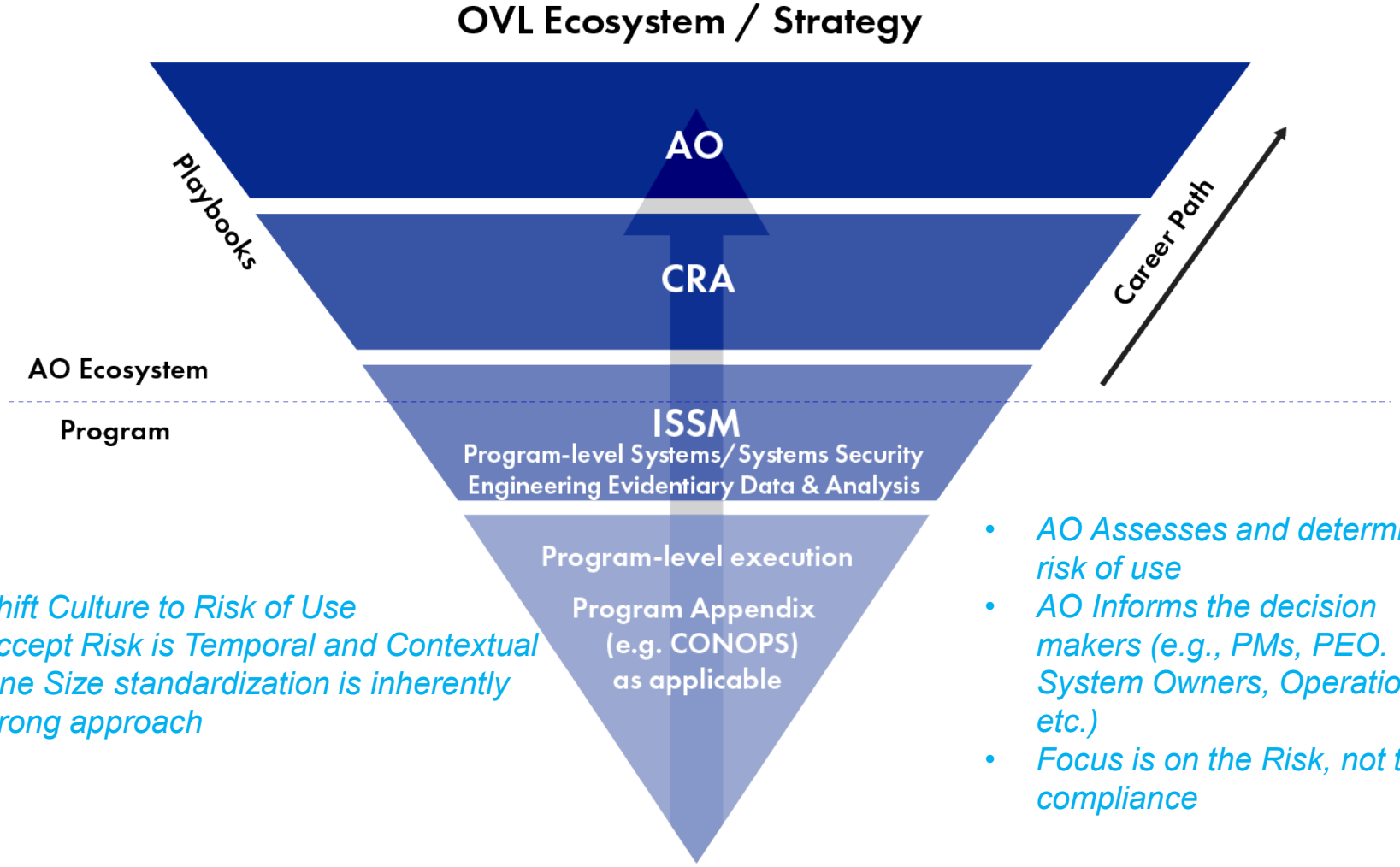
Questions

- What is Continuous Monitoring
- Who is responsible for it?
- Who is responsible for following up on the annotated conditions via the authorization letter?
- How do you keep the AO up to date?
- What is an NSI and who signs off on it?
- What is reciprocity and why is it important?
- Should artifacts be uploaded to eMASS
- Who is responsible for keeping eMASS up to date?

Module 7

Agile Authorization Ecosystem

Operation Vulcan Logic: Agile Authorizations Execution NorthStar



- *Shift Culture to Risk of Use*
- *Accept Risk is Temporal and Contextual*
- *One Size standardization is inherently wrong approach*

- *AO Assesses and determines risk of use*
- *AO Informs the decision makers (e.g., PMs, PEO. System Owners, Operations, etc.)*
- *Focus is on the Risk, not the compliance*

The holistic, continuous authorization ecosystem is focused on Risk of Use.

Operation Vulcan Logic
Fast Track Implementation: Agile Authorizations

1 PHASE

Systems/Systems Security Engineering Evidentiary Data & Analysis

- Architectures
- System Boundaries
- Functional Requirements Decomposition
- Data Flows
- Technologies
- Previous Assessments
- Test Results (Red/Blue/Etc.)

Standard Acquisition Systems Engineering Data

Grow it in

PROGRAM MANAGEMENT

- Facilitate Risk management across S&T, Acquisition, Operations & Sustainment

2 PHASE

Collaboration with AO/CRA

- Discuss risk assessment and way ahead
- Previous assessments analysis results
- Operational Use Perspective

Scope the assessment criteria and outcomes

COLLABORATIVE EXECUTION

- Partnerships with PEO's, DOEs, PMs, S&T, T&E, Sustainers, Users, enables holistic view

3 PHASE

Continually Execute Risk Management

- Tool Agnostic - Focus on Evidentiary Data and Analysis
- Clinically define Risk of Use Posture
- Outline Mitigations for Risks

Starts never ending journey of continuous assessment & monitoring

ENABLERS

- Single, Lead AO for each Weapon System
- Streamline expectations and increase Agility

Operationalizing the Fast Track ATO Process

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
    - Fast Track ATO is key enabler

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

Questions and Discussion

Operation Vulcan Logic

Back Up Slides

Version History

Date	Version	Change Type	Modified By
May 23, 2023	0.1	Initial DOD/CDAO Conversion	M.McLaurin
June 22, 2023	1.0	CDAO update	M.McLaurin

REVISION AND HISTORY PAGE Revisions and version changes to this document are recorded within the above table. New versions are published when changes to the document equate to 10 percent or greater of the document's content, or if a change requires immediate implementation. This record is maintained throughout the life of the document.