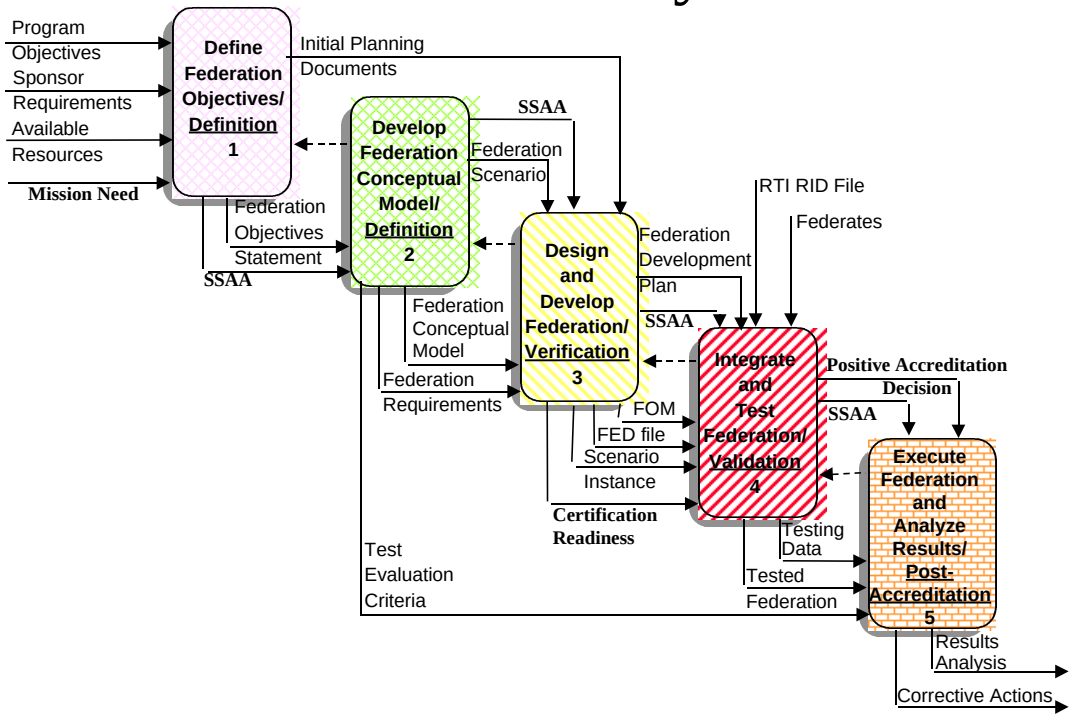
Federation Security Process (overlay for FEDEP)

Philomena M. Zimmerman
Zimmermanpm@navair.navy.mil
(301) 757 - 4624

FEDEP + DITSCAP = FSP

- Federation Security Policy (FSP) is designed to provide a framework in which to address security throughout the FEDEP process.
- Goal is accreditation and secure use of federation
- Split into 5 phases of FEDEP:
  - Define/Document Objectives + Definition
  - Define Real World Domain + Definition
  - Design Federation + Verification
  - Plan Execution/Integrate Federation + Validation
  - Execute/Analyze Outputs + Post Accreditation

Federation Security Process



FSP Phase I

- Start by identifying the mission need - to include functions of system, data outputs, possible candidates.
- Identify Program Manager, User Representative, and Responsible security authority
- Identify type of accreditation - for federation execution, or for federation
- Initiate dialog between all parties
  - consistent and open dialogue from this point on is ESSENTIAL to this process
- Begin the SSAA - a “repository” for security documentation

FSP Phase II

- As work proceeds on conceptual analysis, continue open dialog between DAA, User Representative, Program Manager, and new players as they are identified
- Expect give-and-take among all parties as federation scenario, federation objects, federation relationships, etc. are defined
- Modify the SSAA so it is kept current as details of the federation emerge
- Make sure all parties agree to SSAA modifications / additions

FSP Phase III

- Keep all parties talking. Make sure security representatives are aware of all meetings and meeting outcomes. If they could be present, it would be better as they can provide immediate feedback
- As federates are identified and finalized, ensure all previous decisions and documentation in SSAA are agreeable to all parties. This is a decision point for federate inclusion in federation.
- Data is often the key in security - this is where data to be exchanged is defined
- Keep SSAA current

FSP Phase IV

- Since security personnel have been involved, the tests for certification may be the same tests used (in whole or in part) for federation integration
- Types of certifications achievable (for both federation and federation execution: unconditional, unconditional with identified risks, conditional on modifications, denied
- Modifications to federation are decision of DAA, User Representatives, and Program Manager
- If certification not achieved, Federation Execution cannot proceed

FSP Phase V

- Execution proceeds in secure manner
- Tight configuration control is essential to maintaining accreditation posture
- System modifications may require re-accreditation, and should not be taken lightly
- Once federation is dissolved, accreditation is invalid unless it was achieved for federation. Re-emergence of federation requires reaccreditation
- SSAA becomes repository for all security decisions, etc. and should be put in repository for lessons learned.

Summary

- Goal is accreditation and secure use of federation - not a guarantee
- Goes hand-in-hand with FEDEP
- Expected to work for:
  - geographically distributed and locally contained federations
  - Single or multi-domain federations
- What is lacking?
  - Experience in the process (counting on your feedback)
  - Need to spread the word (especially to accreditors who may be inexperienced in HLA)