DoD Joint Federated Assurance Center (JFAC) 2017 Update

Thomas Hurt
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

20th Annual NDIA Systems Engineering Conference
Springfield, VA | October 26, 2017
Congress and DoD have acknowledged the need for increased software assurance to improve confidence in secure and resilient weapon systems for over a decade.
Joint Federated Assurance Center (JFAC)

FY14 NDAA Section 937—Joint Federated Assurance Center (JFAC)

Key provisions:

- “provide for the establishment of a joint federation of capabilities to support the trusted defense system needs...to ensure security in the software and hardware developed, acquired, maintained, and used by the Department”
- “consider whether capabilities can be met by existing centers”
- “[if gaps] shall devise a strategy [for] resources [to fill such gaps]”
- “[NLT 180 days, SECDEF shall] issue a charter…”
- “submit to congressional defense committees...a report on funding and management”

Charter elements:

- Role of federation in supporting program offices
- SwA and HwA expertise and capabilities of the Federation, including policies, standards, requirements, best practices contracting, training and testing
- R&D program to improve code vulnerability analysis and testing tools
- Requirements to procure manage, and distribute enterprise licenses for analysis tools
What Has DoD Done?

- Development of Concept of Operations (CONOPs) and Charter
- Establishment of JFAC Coordination Center (JFAC-CC), Steering Committees, Working Groups (WGs)
- Piloting Software Assurance (SwA) license distribution and management
- Conduct SwA and Hardware Assurance (HwA) Capability Gap Analysis
JFAC Operational Structure

- **SwA and HwA Working Groups**
  - Collaboration and shared prioritization in daily/weekly activities, meet on a regular basis
  - Recommend policy and guidance
  - Provide community forum for “hard problem” analysis and question/answer

- **JFAC Coordination Center**
  - Coordination of Service Providers
  - Supports programs with situational awareness, information/best practices, coordination
  - SwA analysis tool license distribution
  - Portal: [https://jfac.army.mil](https://jfac.army.mil)
  - Assessment Knowledge Base (future)

- **JFAC Action Officer (AO) WG**
  - AOs for JFAC Steering Committee
  - Maintain enterprise and strategy cognizance
  - Reporting and ROI status
What’s Going On Now?

• JFAC Web portal and SwA tool license distribution

• Security Classification Guide

• Field Programmable Gate Array (FPGA) Strategy

• Resourcing
What’s Next?

- **Develop JFAC Full Operational Capability (FOC) strategy**
  - Improve DoD SwA throughout Lifecycle Planning, Execution and Sustainment
  - Invest in Technology and Resources
  - Upgraded Infrastructure for Federated DoD-wide Coordination of Software Assurance
  - Linking Sustainment to Early Program Development

- **JFAC website on SIPR, JWICS**
  - One-stop shop for SwA tools and best practices
  - New S&T and Assessment Knowledge Base portals
  - https://jfac.army.mil
Conclusion

• **The JFAC’s goal is to provide DoD programs a one-stop shop to request, evaluate, and obtain resources to improve their software assurance practice.**
  – SwA analysis tool license distribution and management
  – Service providers for programs’ SwA work; SMEs focused on hard problems
  – SwA best practices

• **JFAC is addressing key software assurance gaps.**
  – Developing FOC strategy to execute as resourcing becomes available
Systems Engineering: Critical to Defense Acquisition

Defense Innovation Marketplace
http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering
http://www.acq.osd.mil/se
For Additional Information

Mr. Thomas Hurt
ODASD, Systems Engineering
571-372-6129
thomas.d.hurt.civ@mail.mil