Department of Defense Joint Federated Assurance Center (JFAC) Update

Thomas D. Hurt

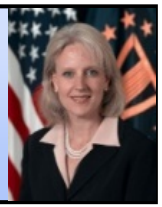
Office of the Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE))

18th Annual NDIA Systems Engineering Conference
Springfield, VA | October 28, 2015

DASD, Systems Engineering

DASD, Systems Engineering - Stephen Welby

Principal Deputy - Kristen Baldwin



Major Program Support
James Thompson

Supporting USD(AT&L) Decisions with Independent Engineering Expertise

- **Engineering Assessment / Mentoring of Major Defense Programs**
- **Program Support Assessments**
- **Overarching Integrated Product Team and Defense Acquisition Board Support**
- **Systems Eng**
- **Systemic Ro**
- **Developmen**
- **Program Protection**

- **System Security Engineering**
- **Software Assurance (SwA)**
- **Hardware Assurance (HwA)**

Engineering Enterprise
Robert Gold

Leading Systems Engineering Practice in DoD and Industry

- **Systems Engineering Policy and Guidance**
- **Technical Workforce Development**
- **Specialty Engineering (System Safety, Reliability and Maintainability, Quality, Manufacturing, Producibility, Human Systems Integration)**
- **Security, Anti-Tamper, Counterfeit Prevention**
- **Standardization**
- **Engineering Tools and Environments**

Providing technical support and systems engineering leadership and oversight to USD(AT&L) in support of planned and ongoing acquisition programs

DoD SwA and HwA Background

2009

❖ NDAA S.254: Trusted Defense Systems Strategy

2011

❖ NDAA S.932: Strategy on Computer Software Assurance

2012

❑ U.S. GAO-12-361: IT Supply Chain. GAO states DoD sets standard for rest of Federal Gov't.

2013

❖ NDAA S.933: Improvements in Assurance of Computer Software Procured by DoD

❑ U.S. GAO 2013 High Risk Report: DOD Weapon Systems Acquisition

2014

❖ NDAA S.937: Joint Federated Centers for Trusted Defense Systems for the DoD

Pre-2009

- Dec 2004: AT&L & NII Establish DoD SwA Tiger Team with the Services and NSA.
- Nov 2005: Established NSA Center for Assured Software

2011

- PPP Outline and guidance implemented
- Formed DoD Trusted Systems & Networks (TSN) Round Table
- POM12 RMD SCRM Study

2012

- DoDI 5200.44: Protection of Mission Critical Functions to Achieve TSN
- Formed DoD SwA Community of Practice (CoP)
- DoD Microelectronics Study Report to Congress

2013

- Interim DoD 5000.02 requires SwA

2014

- NSA Trusted FPGA Study

2015

- Joint Federated Assurance Center (JFAC) Charter
- 937 Report to Congress
- JFAC CONOPS
- Pending: JFAC IOC

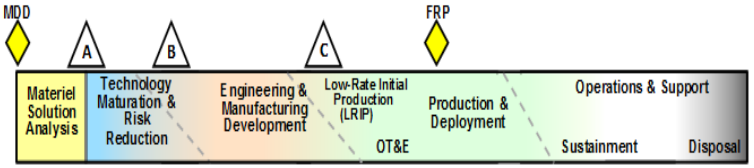
❖ Diamond – Congressional Language ❑ Square – GAO Language • Dot – DoD Action

Sophisticated vulnerability discovery, analysis, and remediation for SW/HW has been a maturing strategic imperative for DoD

Malicious Supply Chain Risk

- ***Threat:***
  - Nation-state, terrorist, criminal, or rogue developer who gains control of ***systems or information*** through supply chain opportunities; exploits vulnerabilities remotely, and/or degrades system behavior
- ***Vulnerabilities:***
  - All systems, networks, and applications
  - Intentionally implanted logic (HW/SW)
  - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
  - Controlled unclassified information resident on, or transiting supply chain networks
- ***Consequences:***
  - Loss of data; system corruption
  - Loss of confidence in critical warfighting capability; mission impact

Access points are throughout the acquisition lifecycle…



…and across numerous supply chain entry points

- Government
- Prime, subcontractors
- Vendors, commercial parts manufacturers
- 3rd party test/certification activities

Malicious Insertion Risk

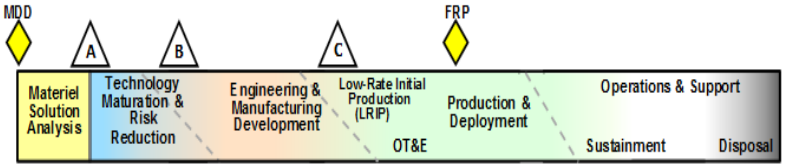
- ***Threat:***

  Nation-state, terrorist, criminal, or rogue entity that attacks systems through vulnerabilities or weaknesses in operational software to disrupt mission, co-opt function, destroy capability, or exfiltrate information

- ***Vulnerabilities:***
  - All systems, including applications and networks
  - Software not adequately assessed and remediated during design, code, and test phases for detectable vulnerabilities and weaknesses
  - Operational software not dynamically evaluated and tested periodically in sustainment to ensure that it continues to function only as intended

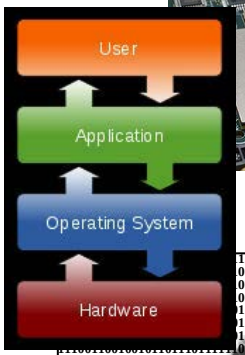
- ***Consequences:***
  - Mission failure
  - Loss of warfighting platforms and systems
  - Critical mission functions co-opted by attacker
  - Loss or degraded mission capability
  - Loss of confidence in system or functions
  - Loss of data and technology

Access points are throughout the acquisition lifecycle…



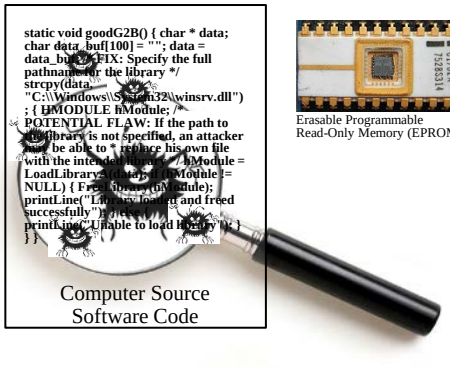
- Program Management
  - Configuration Management
  - Upgrades and Changes
  - Insider Threat
- Operations and Sustainment
  - Prime, subcontractors
  - Vendors, commercial parts manufacturers
  - 3rd party test/certification activities
  - Malicious actors

Joint Federated Assurance Center (JFAC)



Field Programmable Gate Array

Binary Computer Software Code



Computer Source Software Code

Erasable Programmable Read-Only Memory (EPROM)

Assure Mission SW and HW Security

Intent:

- Congress directed DoD to "…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." (FY14 NDAA, Sect. 937)

Expected Outcomes/Deliverables:

- Federated cross-DoD awareness and coordination of software and hardware assurance (SwA/HwA) capabilities, resources, and expertise
- Development and sharing of SwA/HwA vulnerability assessment and remediation best practices, tested tools, and proven processes
- Identification of R&D needs to advance SwA/HwA capabilities for programs in acquisition, operational systems, and legacy systems and infrastructure

Key Participants:

- Sponsor: ASD(R&E)/DASD(SE)
- Stakeholders: CIO, AF, Army, Navy, USMC, NSA, NRO, MDA, DISA, DMEA

Approach:

- Establish DoD-wide federation of SwA and HwA capabilities to meet Congressional intent
- Support program offices across lifecycle by identifying and facilitating access to Department SwA and HwA capabilities, resources, expertise, policies, guidance, requirements, best practices, contracting language, training, and testing support
- Coordinate with DoD R&D and other partners for SwA and HwA technology
- Procure, manage, and distribute enterprise licenses for SwA and HwA automated assessment and analysis tools

Milestones:

Formed Steering Committee and Working Groups	07-2014
Initiated First Series of Technical Tasks	09-2014
Charter signed by Deputy Secretary of Defense	02-2015
Congressional Report signed & submitted	03-2015
CONOPS signed	10-2015
Initiate Capability Assessment, Gap Analysis, Strategic Planning processes	12-2015
Joint Federated Assurance Center IOC	12-2015
JFAC Portal operational	12-2015

JFAC Concept of Operations

Goals

- Operationalize and institutionalize assurance capabilities in support of Program Management Offices and other organizations
- Organize to better leverage the DoD, interagency, and public/private sector capabilities in SwA and HwA
- Collaborate across the DoD to influence R&D investments and activities to improve assurance

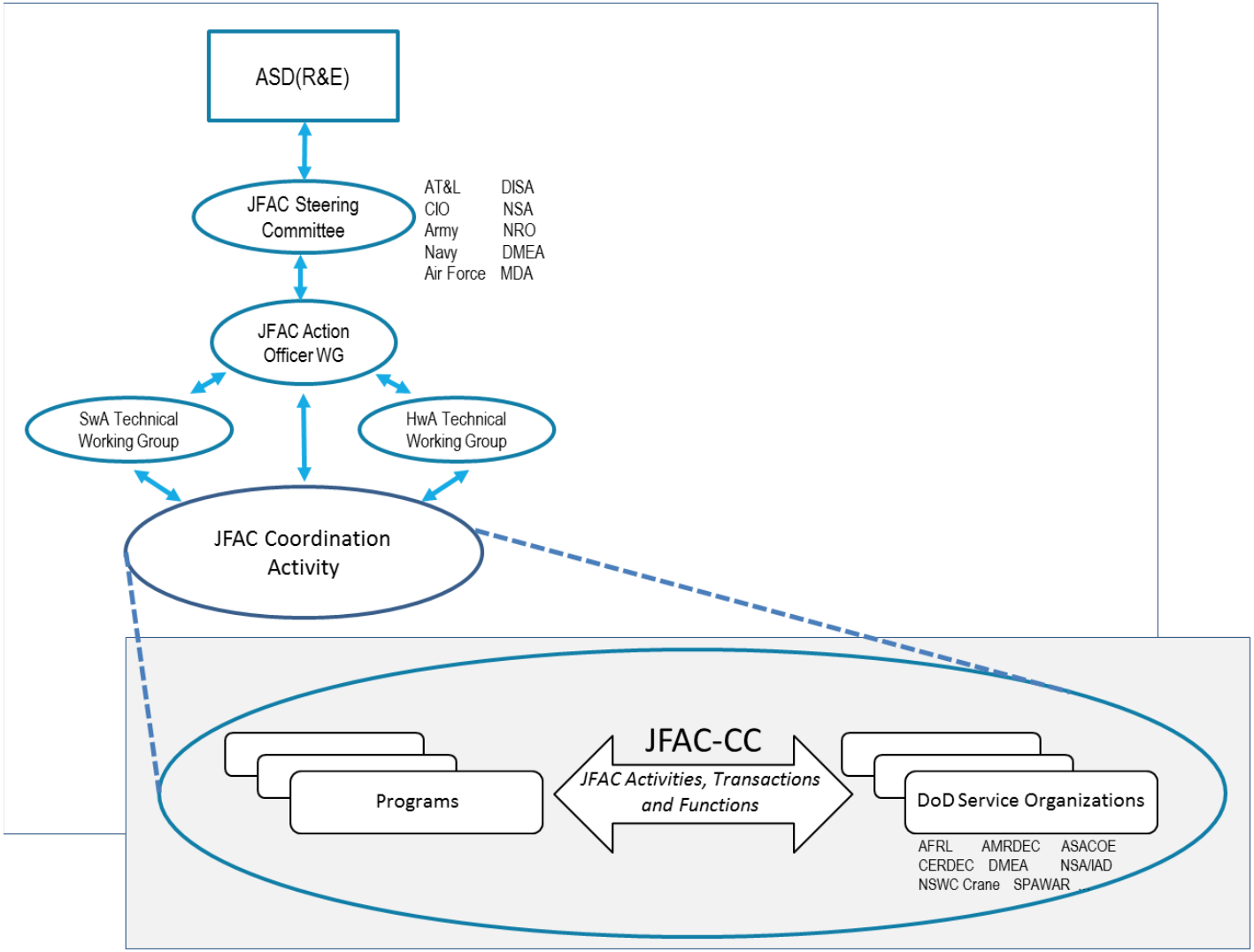
Functions

- Support Program Offices and Systems across the Lifecycle
- Sustain inventory of SwA and HwA resources across DoD
- Coordinate R&D agenda for assurance (hardware, software, systems, services, mission) across DoD
- Procure, manage and enable access to enterprise licenses for selected automated vulnerability analysis and other tools
- Communicate assurance expectations to broader communities of interest and practice (i.e. private industry, academia, other government agencies)

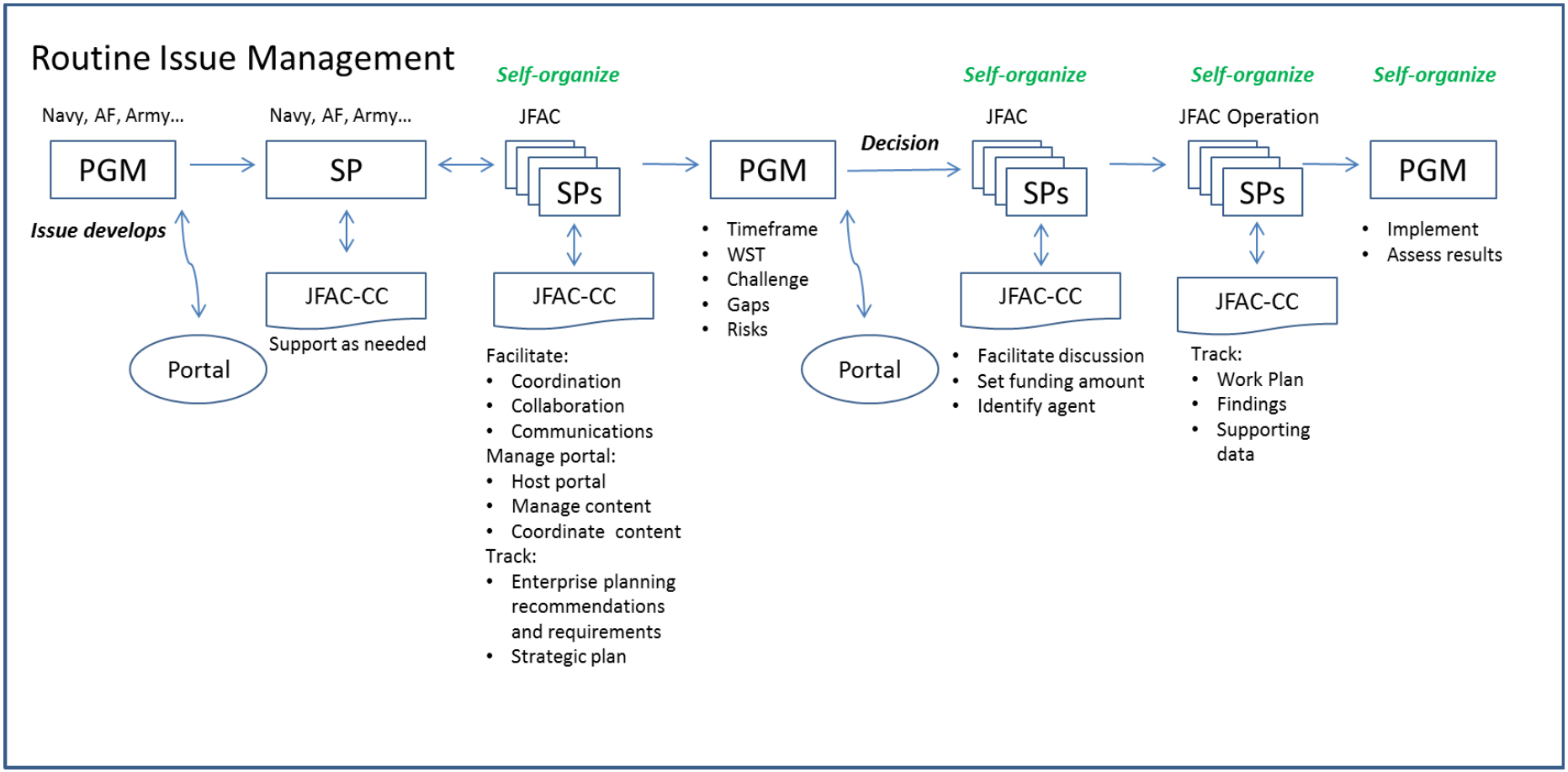
Objectives

- Reduce risk and costs to programs through maturing software and hardware assurance tools, techniques and processes
- Assurance issue resolution through collaboration across the community (federated problem solving)
- Leverage commercial products and methods, and spur innovation
- Incorporate SwA and HwA in contracts for enhanced program protection
- Raise the bar on reducing defects and vulnerabilities though SwA and HwA standardization
- Heighten SwA awareness through outreach, mentoring, training and education
- Assess assurance capability gaps and recommend plans to close

JFAC Organizational Structure



JFAC Example Vignette



JFAC: Way Ahead

- **Program engagement**
  - Foster early program planning for SwA and HwA, architect/design with security in mind
  - Implement risk assessment and mitigation in plans and contracts
  - Thread SwA and HwA activities throughout the lifecycle
- **Community collaboration**
  - Achieve a federated capability to support program needs: including best practices, subject matter expertise, and facilities to address malicious insertion risks
  - Across all DoD SwA and HwA users and providers
  - Partner with Other Government Agencies (OGA)
- **Industry engagement**
  - Develop DoD consensus on approaches to implementing SwA and HwA
  - Dialogue with industry on assurance strategies and approaches
  - Articulation of vulnerabilities, weaknesses, attack patterns, capabilities, countermeasures, and gaps
- **Advocate for SwA and HwA R&D**
  - Tools, techniques, and practices
  - Strategy to increase effectiveness of static and dynamic detection tools
  - Strategy for trusted microelectronics that evolves with the commercial sector
- **People!**
  - Advocate for training, development, and maturation of SwA and HwA competencies
  - Improve awareness, expertise to design and deliver trusted systems

Summary

- **JFAC is a federation of DoD assurance capabilities and capacities**
  - To address current and emerging threats and vulnerabilities
  - To facilitate collaboration across the Department and throughout the lifecycle of acquisition programs
  - To maximize use of available resources
- **Innovation of SW and HW inspection, detection, analysis, risk assessment, and remediation tools and techniques**
  - R&D is key component of JFAC operations
  - Focus on improving SwA and HwA support to programs
- **How can industry help**
  - Continue to improve SW and HW assurance capabilities and methodologies
  - Work with us to develop and maintain SwA and HwA

For Additional Information

Thomas Hurt
Deputy Director, Software Assurance and Software Engineering, DASD(SE)
571-372-6129 | thomas.d.hurt.civ@mail.mil

Systems Engineering: Critical to Defense Acquisition










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

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