Department of Defense (DoD) Joint Federated Assurance Center (JFAC) Overview

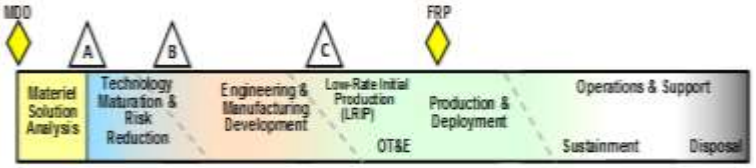
Tom Hurt
Deputy Director, Hardware/Software Assurance
Office of the Deputy Assistant Secretary of Defense for Systems Engineering

ITEA Cyber Meeting, Aberdeen, MD
February 25, 2015

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

DoD SW and HW Assurance 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 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 2016

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
- ❖ Pending: Joint Federated Assurance Center (JFAC) Charter and 937 Report

2016
- ❖ 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

Congressional Direction

403

Business Act (15 U.S.C. 632)) that are awarded contracts by the Department of Defense to assist such businesses to—

(1) understand the gravity and scope of cyber threats;

(2) develop a plan to protect intellectual property; and

(3) develop a plan to protect the networks of such businesses.

SEC. 937. JOINT FEDERATED CENTERS FOR TRUSTED DEFENSE SYSTEMS FOR THE DEPARTMENT OF DEFENSE.

(a) FEDERATION REQUIRED.—

(1) IN GENERAL.—The Secretary of Defense shall provide for the establishment of a joint fed-
tion of capabilities to
ment-wide federa-
pabilities to support the trusted defense system needs of the Department to ensure security in the software and hardware developed, acquired, maintained, and used by the Department, pursuant to the trusted defense systems strategy of the De-

404

partment and supporting policies related to software assurance and supply chain risk management.

(b) DISCHARGE OF ESTABLISHMENT.—In providing for the establishment of the federation, the Secretary shall consider whether the purpose of the federation can be met by existing centers in the Department. If the Department determines that there are capabilities gaps that cannot be satisfied by existing centers, the Department shall devise a strategy for creating and providing resources for such capabilities to fill such gaps.

(c) CHARTER.—Not later than 180 days after the date of the enactment of this Act, the Secretary shall iss
a charter for the federation. The ch

(A) the role of the federation in supporting program offices in implementing the trusted defense systems strategy of the Department;

(B) the software and hardware assurance expertise and capabilities of the federation, including policies, standards, requirements, best practices, contracting, training, and testing;

405

(C) the requirements for the discharge by the federation, in coordination with the Center for Assured Software of the National Security Agency, of a program of research and development to improve automated software code vulnerability analysis and testing tools;

(D) the requirements for the federation to procure, manage, and distribute enterprise licenses for automated software vulnerability analysis tools; and

ts for the discharge by
ation with the Defense
of a program of re-
o improve hardware
esting, and protection tools.

(d) REPORT.—The Secretary shall submit to the congressional defense committees, at the time of the submittal to Congress of the budget of the President for fiscal year 2016 pursuant to section 1105 of title 31, United States Code, a report on the funding and management of the federation. The report shall set forth such recommendations as the Secretary considers appropriate regarding the optimal placement of the federation within the organizational structure of the Department, including responsibility for the funding and management of the federation.

National Defense Authorization Act for Fiscal Year 2014 (NDAA 2014)
Sec. 937 Joint Federated Centers for Trusted Defense Systems for the Department of Defense

NDAA 937 Approach and Status

Congress, through NDAA 2014 Section 937, 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."

Approach:

- **Establish a Federation of HwA and SwA capabilities to support programs in program protection planning and execution**
- **Support program offices across the life cycle by identifying and facilitating access to Department SwA and HwA expertise and capabilities, policies, guidance, requirements, best practices, contracting language, training, and testing support**
- **Coordinate with DoD R&D for SwA & HwA**
- **Procure, manage, and distribute enterprise licenses for SW and HW assurance tools**

Status:

- **Charter under review for DepSecDef signature**
- **937 Congressional Report in process and on track**
- **Working concept of operations, capability map, and capability gap analysis**
- **Initial capability on track for 2015**

Implementing Section 937 through a DoD Joint Federated Assurance Center

Charter Mapping to Section 937 Language

- **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 with NSA Center for Assured Software to improve code vulnerability analysis and testing tools
  - Requirements to procure manage, and distribute enterprise licenses for analysis tools
  - R&D program with DMEA to improve hardware vulnerability, testing, and protection tools

Establishes a Federation of Software and Hardware Assurance Capabilities Across DoD

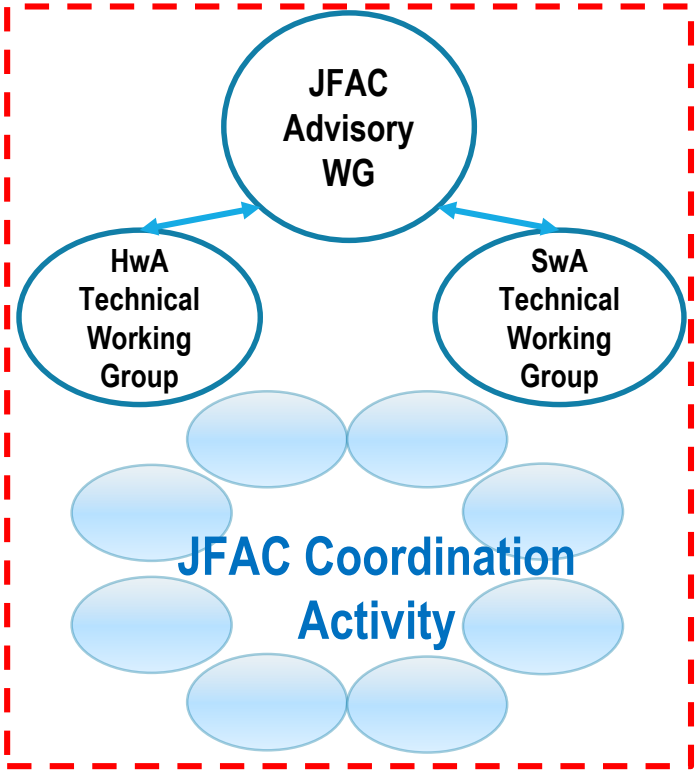
JFAC Goals and Functions

- **Goals**
  - Operationalize and institutionalize assurance capabilities in support of PMOs and other organizations
  - Organize to better leverage the DoD, interagency, and public/private sector capabilities in hardware and software assurance
  - Collaborate across the DoD to influence R&D investments in hardware and software assurance capability gaps
  - Evaluate, over time, the impact of DoD investments and activities in support of assurance
- **Functions:**
  - Support Program Offices and Systems across the Lifecycle
  - Sustain an inventory of SwA and HwA resources across DoD
  - Coordinate the R&D agenda for assurance (hardware, software, systems, services, mission) across DoD
  - Procure, manage and enable access to enterprise licenses for selected automated software vulnerability analysis and other tools
  - Communicate assurance expectations to the broader community

JFAC Stakeholders

- **Steering Committee**
  - USD AT&L
  - DoD CIO
  - Department of Army
  - Missile Defense Agency
  - Department of Navy
  - Defense Information Systems Agency
  - Department of Air Force
  - National Reconnaissance Office
  - National Security Agency
  - Defense Microelectronics Activity
- **Working Groups**
  - Advisory Working Group assigned by above organizations
  - Software and Hardware Working Groups consisting of key service providers
- **Coordination Activity**

Joint Federated Assurance Center



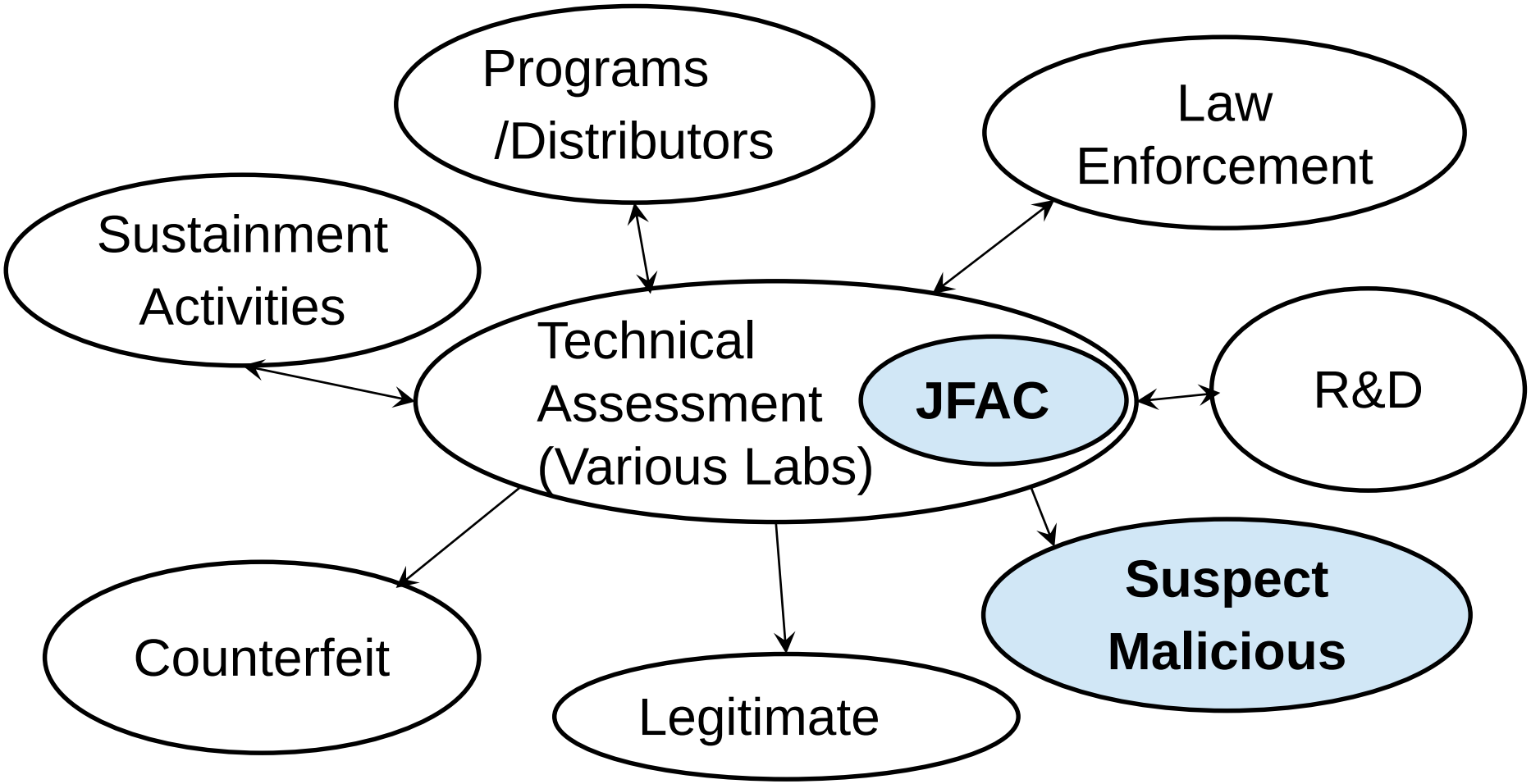
Intent is to federate existing DoD capabilities, ensure sharing of best practices, and provide visibility to programs

JFAC Objectives

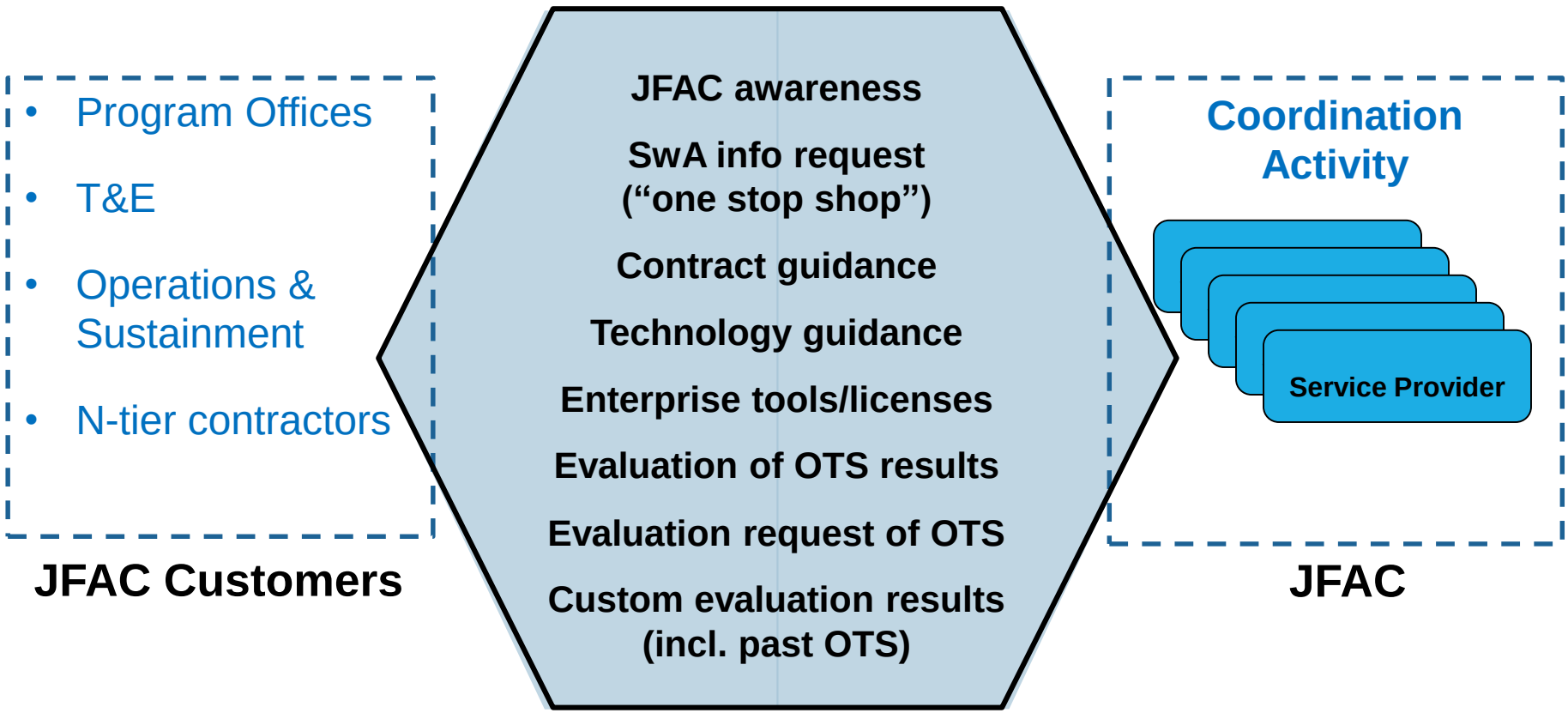
- **Reduce risk and costs to programs through maturing software assurance tools, techniques and processes**
- **Assurance issue resolution through collaboration across the community (federated problem solving)**
- **Leverage commercial products and methods, and spur innovation**
- **Incorporate SwA and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

JFAC Hardware-Focused Customer Interactions

Counterfeit, Re-cycled E-waste, Blacktopped, Potential Malicious, Clones and Substitutions



JFAC Software-Focused Customer Interactions



Summary

- **JFAC is a federation of existing capabilities**
  - To support cross-cutting needs
  - To maximize use of available resources
- **R&D is a key component of JFAC operation**
- **Innovation of SW and HW inspection, analysis, detection, assessment, and remediation tools is vital**
- **How can industry help**
  - Share assurance metrics and best practices
  - Continue to improve SW and HW assurance capability
  - Develop and maintain SW and HW assurance standards

For Additional Information

Thomas Hurt

Deputy Director, Hardware/Software Assurance, 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