Joint Federated Assurance Center Charter

1. PURPOSE AND SCOPE. This charter establishes and describes the Joint Federated Assurance Center (JFAC) mission, functions, construct, and responsibilities in accordance with the Department's Acquisition and Trusted Defense Systems strategy and policy.

2. REFERENCES:

a. Public Law 113-66, National Defense Authorization Act for Fiscal Year 2014, section 937. Joint Federated Centers for Trusted Defense Systems for the Department of Defense

b. Public Law 112-239, National Defense Authorization Act for Fiscal Year 2013, section 933. Improvements in Assurance of Computer Software Procured by the Department of Defense

c. Public Law 111-383, Ike Skelton National Defense Authorization Act for Fiscal Year 2011, section 932, Strategy on Computer Software Assurance

d. Public Law 110-417, Duncan Hunter National Defense Authorization Act for Fiscal Year 2011, section 254. Trusted Defense Systems

e. Interim Department of Defense Instruction (DoDI) 5000.02, Operation of the Defense Acquisition System

f. DoDI 5200.44, Protection of Mission and Critical Functions to Achieve Trusted Systems and Networks (TSN)

g. NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations

3. BACKGROUND. Interim DoDI 5000.02, Operation of the Defense Acquisition System (reference e.), and DoDI 5200.44 (reference f.) define and implement the policy and strategy for TSN within the Department for covered programs. They require program offices to include software assurance (SwA) and hardware assurance (HwA) as part of program protection planning throughout the acquisition life cycle. Program offices and sustaining activities can leverage the JFAC to support the implementation of DoD SwA and HwA requirements.

4. MISSION and OBJECTIVES. The JFAC is the federation of all Department entities having software and hardware assurance capabilities needed by programs. The JFAC will develop, maintain, and offer software and hardware vulnerability detection, analysis, and remediation capabilities through a federation of internal, coordinated organizations and facilities from across the Military Departments, Defense Agencies, and other DoD organizations. The JFAC facilitates collaboration across Science and Technology (S&T), acquisition, Test and Evaluation (T&E), and sustainment efforts to ensure that SwA and HwA capabilities and investments are effectively planned, executed, and coordinated across the Department. The JFAC:

a. Supports 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, training, and testing support.

b. Ensures requirements to innovate software vulnerability analysis, testing, and protection tools are provided to inform DoD R&D strategy development.

c. Ensures requirements to innovate hardware vulnerability analysis, testing, and protection tools are provided to inform DoD R&D strategy development.

d. Establishes and enables efficient and affordable acquisition and use of tools for SwA and HwA analysis and test.

5. JFAC FUNCTIONS. The JFAC:

a. Identifies, promotes, and facilitates access to SwA and HwA capabilities in support of program offices, other DoD, and other Federal Government organizations throughout the acquisition life cycle, to include:

1) Efforts to ensure an inventory of SwA and HwA resources, across DoD, including vulnerability analysis tools;
2) Increasing awareness of vulnerability analysis tools, evidence-based practices, support environments, competencies, threats, and vulnerabilities; and
3) Coordinating access to and capability for applying tools, evidence-based practices, support environments, and expertise across the Department.

b. Acts as the DoD contact for interagency efforts for SwA and HwA policies, guidance, standards, acquisition practices, best practices, training, and testing support.

c. Evaluates, over time, the impact of DoD investments and activities in support of SwA and HwA.

d. Supports Department-level inquiries, studies, and reports regarding SwA and HwA.

6. JFAC MANAGEMENT CONSTRUCT:

a. The JFAC comprises the existing supporting staff and elements selected by the participating DoD Component heads, or their designees, to collaboratively carry out JFAC activities to achieve the Steering Committee's strategies and objectives. Representatives from other Federal Government agencies may be invited to participate in the JFAC.

b. The JFAC Steering Committee includes senior executive representatives from the following DoD Components:

1) OUSD(AT&L)
2) DoD CIO
3) Department of the Army
4) Department of the Navy
5) Department of the Air Force
6) Missile Defense Agency
7) National Security Agency
8) National Reconnaissance Office
9) Defense Information Systems Agency
10) Defense Microelectronics Activity

c. The JFAC Working Group comprises, but is not limited to, the Steering Committee policy and technical representatives with responsibility to accomplish the Steering Committee's strategies and objectives. Additional members may be approved only by the Steering Committee.

7. RESPONSIBILITIES.

a. USD(AT&L) shall:

1) Identify resource gaps, and strategies to mitigate them.
2) Preside at all meetings of the JFAC Steering Committee and associated working groups, and provide administrative management of and support for the JFAC.
3) Integrate JFAC SwA and HwA findings into DoD acquisition policy, guidance, and processes, as appropriate.
4) Assure DoD R&D strategy is informed by SW and HW assurance capability needs.

b. DoD CIO shall:

1) Invite comments from the JFAC when establishing standards and requirements for HwA and SwA to protect DoD information technology.
2) Integrate JFAC findings regarding use of Department SwA and HwA capabilities into cybersecurity policies, guidance, controls, and practices.
3) Collaborate with OUSD(AT&L) to ensure alignment between cybersecurity elements including policies, controls, guidance, and practices, and DoD acquisition elements including policy, guidance, and practices, for SwA and HwA.

c. JFAC Steering Committee shall:

1) Develop the JFAC vision, goals, and objectives, provide oversight, and maintain accountability.
2) Review and approve the JFAC concept of operations (CONOPS), as required.
3) Review JFAC capability gap analysis and approve needed modifications.

d. JFAC Working Group shall:

1) Develop and update the JFAC CONOPS, as required.
2) Oversee operational execution of the JFAC.
3) Use JFAC performance and metrics to determine and report return-on-investment, as required.
4) Assess JFAC capabilities and capability gaps and recommend mitigations, as required.
5) Resolve conflicting policies, schedules, and priorities.

e. JFAC supporting staff shall:

1) Execute the JFAC CONOPS, which includes performing SwA and HwA tasks and conducting capacity gap analyses.
2) Support development of and updates to the JFAC CONOPS and JFAC operation, as required.
3) Recommend and supply metrics for JFAC performance and SwA and HwA.
4) Identify and maintain cognizance of JFAC operational capabilities and capability gaps, including resources needed to address the gaps, by priority.
5) Identify and analyze reported vulnerabilities in software and hardware, including systemic patterns of causation and mitigation approaches across DoD for covered programs, and other systems as appropriate, across the life cycle.
6) Monitor effectiveness of software tools and techniques, and provide data as required.
7) Interact with program offices in accordance with each DoD Component's communication plan.

f. Participating DoD Components shall:

1) Provide SwA and HwA capabilities and resources, and support for the JFAC and management construct.
2) Assist in the formulation of JFAC operational requirements.
3) Develop R&D budget requirements in coordination with the JFAC.
4) Nominate SwA and HwA capabilities and sustain inventory.
5) Develop a communication plan to manage interactions between the JFAC support staff, members and program offices.
6) Provide SwA and HwA capabilities to DoD programs and interact with program offices in accordance with each DoD Component's communication plan.
7) Execute the JFAC CONOPS based on direction and resources.

g. DMEA shall:

1) Coordinate with the office of the Deputy Assistant Secretary of Defense (Research and Development) (DASD(RD)) on requirements for the DoD R&D strategy to improve hardware vulnerability, testing, and protection tools.

h. NSA shall:

1) Coordinate with the Office of the DASD(RD) on requirements for the DoD R&D strategy to improve hardware and software vulnerability detection, analysis, testing, and protection tools, and
2) Support the JFAC Working Group with SwA and HwA subject matter expertise

This charter becomes effective upon signature and remains in effect until revised or rescinded.

Robert O. Work
Deputy Secretary of Defense

9 February 2015
Date