RY17-1

Cyber Physical System Assessment tools and techniques for Trusted Microelectronics

1. **Research Title:** *Cyber Physical System Assessment tools and techniques for Trusted Microelectronics*

2. Individual Sponsor:

AFRL/RYW
Mr. Matthew Casto
AFRL/RYWA
2241 Avionics Circle, Bldg 620
WPAFB, OH 45433-7333
Matthew.Casto@us.af.mil

3. Academic Area and Education Level: Electrical & Computer Engineering/Mixed-Signal and Formal Verification (Ph.D. Level)

4. Objectives: The primary objective of this research is to develop a taxonomy of hardware vulnerabilities and fault generators that are representative models of hardware Trojan components potentially inserted into FPGAs, digital application specific integrated circuits and/or mixed-signal integrated circuits. Vulnerabilities will be enumerated and ranked in priority as a vulnerabilities list. Hardware Fault Pattern (HFP) generations of vulnerabilities needs to be developed similar to what has been established for software common weaknesses and common vulnerabilities. With a ranked vulnerability enumeration list developed, techniques of Formal and Test-bench Verification may be developed and applied for the purpose of evaluating an FPGA or fabricated integrated circuit's integrity to the original design specification, to include quantifiable metrics relating levels of trust.

5. Description: As microelectronics continues to advance in their complexity and to be purchased from varied supply chains, there is an increased concern of integrated circuits containing hardware Trojans (malicious bugs) or fabrication faults that would compromise the integrity of the original chip functionality. Currently, there is not a well-established methodology for verifying that the outsourced design accurately represents the fabricated chip. As a result, there is an increasing concern regarding the level of trust one can have in the fabricated chip once it has been received back from the foundry, namely if the chip is fully equivalent to the original design without additional, degraded, or auxiliary functionality. In the same manner that software Trojans were developed out of malicious intent in order to compromise computer systems, hardware Trojans are starting to become more prevalent in literature and the chip manufacturing industry. The varied and sometimes unknown supply chain presents many opportunistic points in the manufacturing flow for Trojan insertion. The scope of the trusted microelectronics research involves developing a taxonomy or classification of hardware vulnerabilities and fault generators and Trojans that can be used to develop statistical assessment fault models. These fault models would then be employed for establishing metrics for evaluating design integrity.

6. Research Classification/Restrictions: This work is unclassified; U.S. Citizens only.

Distribution Statement A – Approved for public release by 88ABW-2016-3469. Distribution is unlimited.

7. **Eligible Research Institutions:** Indicate to what organizations this topic should be provided

☒ **DAGSI** (Wright State University, AFIT, Ohio State University, University of Dayton, Miami University, Ohio University, University of Cincinnati) NOTE: Topics submitted to DAGSI must be approved for public release. Need PA Approval #

☐ **AFIT** (only)

☐ **USAFA** (only)

If you are submitting a topic for the USAFA, indicate if you are also interested in sponsoring a USAF Cadet in summer 2015 (Average cost for USAF Cadet for 33 days is $5000)

☐ Yes ☐ No

Distribution Statement A – Approved for public release by 88ABW-2016-3469. Distribution is unlimited.