

ATTN: Networking and Information Technology Research and Development (NITRD) program representatives

Thank you for the opportunity to respond to your Request for Information (RFI) for the Five-Year Strategic Plan for the NITRD program. My responses for the RFI include:

- **Multi-core Software Development Tools** – Currently there are few debugging tools for multi-core software development. For instance, improved software debugging methods for multi-core chips is needed. For debugging a software error, the engineer must uncover the processing interactions between the multiple cores that caused the error. Today's current debugging tools can provide insight into an individual core's processing, but these tools are incapable for providing insight to every core's processing simultaneously. Also, additional communication protocols and tools are required for improved inter-core communication for multi-core chips. Many current communication protocols like TCP/IP are designed for very specific environments. The inter-core communication environment requires very fast communication speeds over short distances of less than a few inches over silicon.

The desired result is for a suite of software engineering tools that allow for easy and convenient multi-core software development. The multi-core software debugging tools should allow software developers to simultaneously debug all threads operating on the multiple cores with each core processing synchronously with the other cores on the micro-processor. One or more communication protocols and tools would be developed for very fast inter-core communication for multi-core chips. Multiple protocols and tool suites may be required for differing chipset design.

To develop these tools, there should be a multi-disciplinary approach involving academia, software vendors, and hardware vendors. The National Sciences Foundation (NSF) and similar research and development organizations such as the Air Force Research Laboratory (AFRL) should provide program leadership and research direction.

- **Validation/Verification and Certification of Multi-core chips** – Certifying systems comprised of uni-core hardware architectures is very difficult. Now, new certification methods must be devised for multi-core chips. Multi-core chips have the following certification issues:
  - The multiple cores on a microprocessor share L2 cache memory. To certify multi-core chips, techniques and methodologies must be developed to ensure that no core is able to over-write another core's L2 cache memory.
  - In a real-time operating system (RTOS) executing on a multi-core system, a thread is scheduled to execute. Only core 1 is available for executing the thread, so the thread executes on core 1. The next time the thread is scheduled to execute several cores are currently not utilized, which core will the thread execute on? Techniques and procedures must be developed whereby thread execution is predictable and consistent for the system's overall execution.

The certification, validation, and verification of embedded systems has become extremely expensive as our computer systems become more complex. In 2007, 40% of all processors that Intel shipped contained multiple cores. By 2011, it is expected that 95% of all processors that Intel ships will contain multiple cores. Similar multi-core migration trends are being seen with other microprocessor manufacturers. The sooner that research

organizations begin investigating validation/verification and certification for multi-core chips, the better off the computer industry will be.

To develop these certification techniques and methodologies, there should be a multi-disciplinary approach involving academia, software vendors, hardware vendors, and the National Security Agency (NSA). The NSA, NSF, and similar research and development organizations such as the Air Force Research Laboratory (AFRL) should provide direction and program leadership.

- **Architecture and Implementation Security Vulnerability Discovery** – To reduce the effects of viruses and mal-ware, many network devices execute Intrusion Detection/Prevention software. Many Intrusion Detection/Prevention packages are very good but they require frequent updates to stop the latest viruses and mal-ware. Furthermore, these tools eat up valuable processing time that the software applications they are protecting should be using. It would be beneficial to generate tools that identify security vulnerabilities while developing a system's architecture and code. The earlier these security vulnerabilities are discovered and solutions are developed to fix the vulnerabilities, the less expensive the overall system will be. To develop these Architecture and Implementation Security Vulnerability Discovery techniques, methodologies, and tools, there needs to be a multi-disciplinary approach involving academia, software middleware vendors, software operating system vendors, hardware vendors and the NSA. The NSA, NSF, and similar research and development organizations such as the Air Force Research Laboratory (AFRL) should provide program leadership and direction.