High Confidence Software and Systems (HCSS)

NITRD Agencies: NSF, NIH, DARPA, NSA, NASA, NIST, OSD
Other Participants: AFRL, ARO, DHS, FAA, FDA, ONR

HCSS activities focus on the basic science and information technologies necessary to achieve affordable and predictable high levels of safety, security, reliability, and survivability in U.S. national security- and safety-critical systems. These activities are essential in domains such as aviation, health care, national defense, and infrastructure.

President's 2006 Request

Strategic Priorities Underlying This Request

- Assuring the security, safety, and highly dependable performance of systems and software in critical applications and U.S. infrastructures is one of the most significant and difficult challenges in computing and networking R&D. The technical complexity of these systems continues to grow rapidly in two directions – ever-larger systems of systems involving many millions of lines of code and ever-smaller embedded systems and networks of such systems. As of 2005, the NITRD research community is in the third year of an intensive focus on software and systems assurance arising not only from the new national security climate but also from the rapid emergence of embedded sensor applications in industry; the growing need for secure, reliable IT systems in health care informatics and medical devices; and the increasing complexity of large-scale systems of systems such as the U.S. financial system.
- Agencies' 2006 plans reflect their search for new science-based concepts, technologies, and tools that can revolutionize not only the engineering processes for construction, testing, and certification of software, but also the overall engineering of systems to incorporate high assurance levels at every stage of system design – a new concept in IT R&D. The new area of hybrid and embedded systems such as medical devices offers a rare opportunity to instantiate high assurance from the beginning, not just re-engineer legacy systems.

Highlights of Request

- **NSF:** Develop a new Computer Systems Research program in basic and technology research for high-confidence embedded systems, hybrid control, distributed systems; continue Cyber Trust and Science of Design themes across the divisions of CISE Directorate
- **NSF, DHS:** Continue DETER/EMIST network testbed and experimental framework for network security research launched in 2004
- **DARPA, NSF:** Continue four jointly funded, multi-university projects in Cyber Trust that are developing methods for demonstrating that large software systems are free from flaws
- **NSA, NSF, with NASA, NIST, and other HCSS participants:** Initiate a jointly funded research project on assured and composable, secure, real-time operating systems and middleware. The project will develop an integrated systems and verification technology base for assured systems that are component-oriented, configurable, and coordinated. The goal is to enable future distributed, real-time, embedded systems that have security and assurance built in "from the ground up."
- **NSA, NSF, with other HCSS agencies:** Verification Grand Challenge Workshop planning
- **NIST:** New activity in high-confidence methods for voting and vote counting

Planning and Coordination Supporting Request

- **HCSS CG and agencies:** Two-part High Confidence Medical Device Software and Systems (HCMDSS) activity – November 2004 workshop planning meeting; June 2005 national workshop on improving design, certification, and operation (by both health care professionals and consumers) of medical device software and systems that will result in better and more cost-effective medical care
- **HCSS CG, FAA:** Aviation workshop planning meeting and workshop to address safety issues in certification of autonomous vehicles and air traffic management; goal is to formulate a research agenda that addresses safety and security and is compatible/compliant with civilian processes.

- **DARPA, NIST, NSF, FAA, ONR:** Support for NA/CSTB Cyber Security study
- **NSA, NSF, ONR, with participation by DARPA, NASA, NIST, ARO, FAA, FDA:** NA/CSTB study on "Sufficient Evidence? Building Certifiably Dependable Systems" to assess current practices for developing and evaluating mission-critical software, with an emphasis on dependability
- **NSA, NSF, with NASA, NIST, other HCSS participants:** Collaborative study and planning for 2006 initiative for a real-time research operating system using open systems technologies
- **NSA, NSF, with HCSS agencies:** Planning workshop for Software Verification Grand Challenge conference
- **NSA, with participation by other HCSS agencies:** Fifth annual HCSS conference in Spring 2005 to showcase recent technical accomplishments, promising research activities, and future research directions, all focused on improving the confidence of software and systems
- **NIST, with participation by other HCSS agencies:** Workshop on Software Assurance Metrics and Tools Evaluation
- **FDA:** Collaborations on medical device safety, including with NSF on proton beam and with NSA on unintended function checker

2005- 2006 Activities by Agency

NSF: Cyber Trust – cyber security foundations, network security, systems software, information systems; Science of Design – assured design for software-intensive computing, information, and communications systems; ITR – IT and high-confidence hybrid control systems for critical infrastructures such as the power grid, open source/open verification technology; Computing Processes and Artifacts and Computing Systems Research – assured platforms and software, and distributed, real-time, embedded computing; computational models and assurance methods for safety-critical systems
DARPA: Self-Regenerative Systems effort to develop systems able to function fully in spite of attacks; Security-Aware Critical Software program (new in 2005) to create software that provides a comprehensive picture of security properties and current status, presenting this information at multiple levels of abstraction and formality
NSA: R&D in trusted development (ways to achieve assured software and system designs with assured development techniques throughout the software lifecycle) and containment (mitigating risks of systems whose components are not assured); research in transparency (development of critical architectures and components necessary to support information assurance) and high-assurance platform (supporting promising partnerships through the development of new platform-level containment mechanisms and measurement capabilities)
NASA: Automated mathematical techniques for high-confidence software development; Highly Dependable Computing Platform (HDCP) Testbed (evaluating real-time in-flight software demands); Mission Data Systems reusable software infrastructure for 2005 Mars mission; R&D in software engineering, assurance, and verification and validation techniques for mission-critical applications. Some aviation safety and security projects end in 2005, including efforts in flight-critical systems; 2006 projects currently being planned. The AuRA project is exploring advanced technologies for autonomous aircraft, including efforts to ensure integrity of underlying computational capabilities.
NIST: Continue work in e-commerce, e-health, computer forensics, test method research, security technologies, systems and network security, management and assistance, and security testing and metrics; lead DHS and DoD efforts to create studies and experiments to validate existing software assurance metrics and develop new metrics

AFRL: Developing the safety and security certification requirements for future Air Force applications of unmanned aerial vehicles; forming multi-technical directorate team to participate in and contribute to a national investment strategy plan; workshop planning meeting and full workshop anticipated in 2005
FAA: Developing a rapid quarantine capability; testing biometrics single sign-on; testing behavior-based security; developing an information systems security architecture; establishing an integrity and confidentiality lab to test wireless information systems security; extending COCOMO II (COnstructive COst MOdel II) to include security; validating Web data mining to find FAA vulnerabilities
FDA: Research projects include: proton beam therapy device (safety and modeling); software for an infusion pump with a control loop, which led to an initiative of similar control loop software for a ventilator device (certification); blood-bank software regulation (certification); reverse engineering of C programs to look for inconsistencies and errors in radiation treatment planning systems used in tumor treatment (forensics); unintended function checker (forensics)