High Confidence Software and Systems

Definition of HCSS PCA

The activities funded under the High Confidence Software and Systems (HCSS) PCA 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 systems play key roles in critical domains such as aviation, health care, national defense, and infrastructure. Many complex software-and information-intensive systems that have high consequences of failure must be certified as to their safety and security. Currently, however, this certification – even when possible at all – requires overwhelming cost, time, and effort, discouraging and delaying innovation of new technologies and processes. The overall HCSS goal, then, is to develop and demonstrate revolutionary capabilities for system development and assurance that balance and reduce risk, cost, and effort to achieve systems that behave in predictable and robust ways. HCSS R&D will help transform our ability to feasibly build certifiably dependable systems in the challenging environment of an increasingly interconnected and automated society.

Broad Areas of HCSS Concern

- Security and privacy
- Safety, robustness, reliability of software and systems
- Trust, risk, and accountability
- Assured development and certification of software and systems
- Survivability

Technical Goals

- Provide a sound theoretical, scientific, and technological basis for assured construction of safe, secure systems
- Develop hardware, software, and system engineering tools that incorporate ubiquitous, application-based, domain-based, and risk-based assurance
- Reduce the effort, time, and cost of assurance and quality certification processes
- Provide a technology base of public domain, advanced-prototype implementations of high confidence technologies to enable rapid adoption
- Provide measures of results

Illustrative Technical Thrusts

- Foundations of assurance and composition
- Correct-by-construction system design and software technologies
- Evidence and measurement technologies for verification and validation
- Authentication, access control, intrusion detection, trust models, and forensics
- Dependable open, distributed, and networked systems
- Secure and reliable hardware, network, operating system, and middleware technologies
- Dependable and survivable real-time, embedded, and control system technologies
- Verification and certification technologies
- Dependable technologies for transportation, medical

HCSS Agencies

NSF	NASA	NIST
NSA	DARPA	NIH

Participatimg Agencies

AFRL FAA FDA ONR

HCSS PCA Budget Crosscut

FY 2004 Estimate	FY 2005 Request
$144.4 M	$152.5 M

devices and health systems, power generation and distribution systems, financial services, and other critical infrastructures

- Experimentation and reference HCSS implementations
- Assured open source software

HCSS PCA: COORDINATION AND ACTIVITIES

HCSS HIGHLIGHTS

In FY 2001, the word "Software" was added to the name of the prior High Confidence Systems PCA to reflect the central role played by software in the overall reliability, security, and manageability of the Nation's most complex and critical computing and communications systems. The recommendation to make software a top priority of Federal IT R&D activities had been highlighted by the PITAC in its 1999 report on Federal IT R&D investments. The purview of the High Confidence Software and Systems PCA now includes R&D in all aspects of software development for very-high-assurance trusted systems.

Through monthly meetings, the HCSS Coordinating Group (CG) shares information on agency research programs, upcoming meetings, and workshops. The group cooperatively supports studies on HCSS topics, holds workshops in key research and programmatic areas, and invites other agencies to conferences and principal investigator (PI) meetings. FY 2004 CG activities include:

- A study on "Sufficient Evidence? Building Certifiably Dependable Systems" being conducted by the Computer Science and Telecommunications Board of the National Academies. Sponsored by NSF, NSA, and ONR; AFRL, ARO, DARPA, FAA, FDA, NASA, and NIST also participate. The study brings together a broad group of experts to assess current practices for developing and evaluating mission-critical software, with an emphasis on dependability objectives. The group is addressing system certification and examining a few application domains (e.g., medical devices and aviation systems) and their approaches to software evaluation and assurance. The goal is provide some understanding of what common ground and disparities exist. The study committee hosted a workshop on Software Certification and Dependability on April 19-20, 2004, to survey technical, business, and governmental perspectives and to promote dialogue between the research community and government and industry practitioners who develop safety-critical systems.
- The HCSS CG hosted an Open Verification Workshop on April 12, 2004.
- Several other HCSS agencies participated in NSA's High Confidence Software and System Conference, April 13-15, 2004.
- A set of aviation safety workshops is being planned to address safety issues related to the use of unmanned aerial vehicles in civilian and military airspace. AFRL, FAA, NASA, and NSF are the major planners.
- The HCSS CG is planning a workshop on medical devices software safety, with FDA, NASA, NIST, NSA, NSF, and others.

MULTIAGENCY COLLABORATIONS

In FY 2004, HCSS agencies are working together on several collaborative research projects and workshops in assurance, cybersecurity, and medical devices. For example:

- Using a new NASA testbed facility, NSF and NASA are jointly sponsoring the Highly Dependable Computing and Communications Systems Research (HDCCSR) program to promote the ability to design, test, implement, evolve, and certify highly dependable software-based systems.
- DARPA, NSF, and other agencies supported the 2003 kickoff of the Embedded Software Consortium for Hybrid and Embedded Software and Systems (ESCHER, which is included in both the HCSS and SDP PCAs). This group, which has industry support and participation, will focus on system design tools, open source system software, and reference implementations.
- NSF is supporting a cybersecurity study by the Computer Science and Telecommunications Board (CSTB) of the National Academy of Science and invites participation by other agencies.
- FDA and NSF are exploring a joint project to promote participation by computer-science students at FDA. Students will work to facilitate the transition of software methods and to expand FDA's expertise in identifying needs for software-enabled medical devices.

HCSS R&D Programs By Agency

Selected FY 2004 Activities and FY 2005 Plans

HCSS NSF HCSS

NSF's HCSS activities reside in the Cyber Trust and Science of Design themes in the Computer and Information Science and Engineering (CISE) Directorate, and in the NSF-wide Information Technology Research (ITR) Program as follows:

Cyber Trust – initiative across CISE divisions that envisions a society in which:

- Computing systems operate securely and reliably
- Computing systems protect sensitive information
- Systems are developed and operated by a well-trained and diverse workforce

This program supports research on foundations, network security, systems software, and information systems. It sponsors integrated education and workforce activities. Cyber Trust workshops, including PI workshops, are open to participants from other government agencies. In other current research efforts, NSF is seeking help from other agencies in identifying technology transfer opportunities and creating and distributing relevant cyber trust data sets.

Science of Design – a crosscutting initiative that emphasizes design of software-intensive computing, information, and communications systems. The goal is to improve the development, evolution, and understanding of systems of large-scale scope and complexity. These are systems for which software is the main means of conceptualization, definition, modeling, analysis, development, integration, operation, control, and management. A workshop was held November 2-4, 2003, in Northern Virginia to develop the program's foundations.

ITR Program – emphasizes national priorities including national and homeland security, which includes research related to critical infrastructure protection and SCADA systems.

Other CISE program activities – CISE's Distributed Computing, Embedded and Hybrid Systems, Networking, and Foundations of Computing Processes and Artifacts programs also include HCSS work.

The following current projects are representative of NSF support for efforts addressing aspects of trustworthy systems:

- Cryptography
  - Information Theoretic Secure Hyper-Encryption and Protocols
- Data, Security, and Privacy
  - DataMotion: Dealing With Fast-Moving Data
  - Deployment-Oriented Security and Content Protection
  - Sensitive Information in a Wired World
- High Confidence Control
  - A Unified Framework for Distributed Control with Limited and Disrupted Communication
  - Algorithmic Synthesis of Embedded Controller
  - Symbolic Approaches to Analysis and Hybrid Systems
- Prevention, Detection, and Response
  - A Semantic-Based Approach for Automated Response to Attacks
  - Architectural Solutions for Preventing Distributed Denial of Service Attacks
  - Automated and Adaptive Diversity for Improving Computer Systems Security
  - Forensix: Large-scale Tamper-resistant Computer Forensic System
  - Intrusion Detection Techniques for Mobile Ad Hoc Networks
- Systems Software for Protecting Critical Infrastructure
  - Distributed Authentication and Authorization: Models, Calculi, Methods
  - High-Assurance Common Language Runtime
  - Key Management for Secure Dynamic Group Communications
  - Language-Based Software Security
  - Practice-Oriented Provable Security for Higher-Layer Protocols: Models, Analyses and Solutions
  - Security and Privacy for Publish-Subscribe Systems
  - Survivable Trust for Critical Infrastructure
  - Trusted Peer-To-Peer Systems

In FY 2005 , NSF will continue HCSS R&D in:

- *Cyber Trust – research aimed at creating systems that are more predictable, more accountable, and less vulnerable to attack and abuse; developed, configured, operated, and evaluated by a well-trained and diverse workforce; and used by a public educated in their secure and ethical operation*
- *Disciplinary research in science and technology for the design and implementation of high-confidence networks, embedded and control systems, computer hardware design, operating systems, and distributed systems. CISE will also support research in assurance technology and methods that help to verify safety, security, timeliness, and correctness aspects of critical systems*
- *Research projects under ITR aimed at dramatically increasing our ability to build high-confidence security- and safety-critical systems*

Selected new multiyear project awards made in August 2004 include:

- *Byzantine Fault Tolerance for Large-Scale, High-Performance Distributed Storage Systems*
- *The Design and Use of Digital Identities*
- *Graph-Based Refinement Strategies for Hybrid Systems*
- *IIT-based Collaboration framework for Preparing against, Responding to and Recovering from Disasters involving Critical Physical Infrastructures*
- *Panoply: Enabling Safe Ubiquitous Computing Environments*
- *Privacy-Preserving Data Integration and Sharing*
- *Toward a Multi-Layered Architecture for Reliable and Secure Large-Scale Networks: The Case of an Electric Power Grid*

HCSS NSA HCSS

Information Assurance Research Group (IARG) – promotes HCSS research through three product-assurance capability threads:

- Trusted by design – to help software engineers achieve assured designs and reduce the cost of certifying the security of complex information systems
- Trusted by analysis – to assess the confidence in a system that has been built outside of NSA control and whose assurance is unknown
- Containment – to balance granularity of protection against ease of use and cost

The HCSS roadmap for IARG comprises three areas of research:

- **Foundations to develop the supporting theory and scientific basis for high-confidence systems** such as automatic theorem proving, design and analysis of protocols, interoperability and composition and decomposition of agents, and systems security and survivability architectures. Current work includes:
  - National Academy of Sciences Certification Study, focused on addressing system certification and approaches to software evaluation and assurance.
  - Protocol Specification and Synthesis, effort focused on foundational methods of secure communication, with the goal of providing methods and tools upon which the design, analysis, and implementation of security structures might be carried out.
- **Tools and technologies for building high-confidence systems of the future** through the development of analysis, evaluation, and vulnerability tools and techniques. Projects include:
  - Specware, an environment supporting the design, development, and automated synthesis of correct-by-construction software
  - Cryptol, a programming language focused solely on the domain of cryptography, and recently adopted by General Dynamics
  - Vulnerability discovery, focused on developing and demonstrating a support environment for the analyst who is interested in software system vulnerabilities
  - Java Program Verification Condition Generator, a tool that uses formal analysis to eliminate classes of errors during software development of Java programs
  - Formal analysis of hardware/software co-design
  - Biospark, reliability engineering in biometrics that teams HCSS, smart card, and biometrics researchers
  - Polyspace, a project focused on evaluating the fitness for use of the commercial Polyspace static verifier for detecting run-time software errors
- **Engineering and experimentation to demonstrate the effectiveness and efficiency of HCSS technologies** on diverse hardware and software

platforms. Projects include the following:

– Trusted Web server, focused on developing a cross-domain server that can be certifiable for simultaneous connection to networks spanning two or three domains

– Osker (the Oregon Separation Kernel), a prototype POSIX-compliant operating system in Haskell (see the next bullet) that provably achieves a strict separation between processes according to a specified security model. Osker is a challenge application for the Programatica project, a system for developing high-assurance software.

– Haskell on Bare Metal (HBM), an adaptation of the Haskell runtime system, to replace the usual operating system layers between application and hardware

– Java applet generation, an automatic generator that produces Java Card applets from high-level formal specifications

– AAMP7 development environment, a partition-aware development environment for Rockwell Collins's AAMP7 microprocessor that will allow rapid development of partitioned AAMP applications

NSA's FY 2005 planned activities in HCSS include:

- *Host 5th Annual HCSS Conference*
- *Continue joint sponsorship of National Academy of Sciences study on software certification*
- *Initiate joint sponsorship of Open Verification activities with HCSS CG members, resulting in sponsorship of IFIP working conference of Verified Software as well as a Safe Code workshop*
- *Sponsor and conduct research through NSA IARG within the following research themes:*
  - *Product assurance: HCSS tasks focused on trusted development and containment mechanisms*
  - *Trusted Development Thread, which attempts to achieve assured software and system designs and implementations through enhancement of assured development and analysis techniques throughout the entire software and system lifecycle*
  - *Containment Thread, which is focused on mitigating the risk posed by our inability to build systems whose components are all perfectly assured, thereby limiting the impact of improper software and system behavior. The primary challenge in designing containment mechanisms comes in balancing granularity of protection against ease of use and cost.*
  - *Transparency: HCSS task focused on supporting the development of critical architectures and components necessary to support information assurance*
  - *High Assurance Platform: HCSS tasks focused on supporting very promising industrial partnerships through virtualization and measurement capabilities*

HCSS NASA HCSS

NASA missions have several critical needs that HCSS R&D helps address:

- Mission- and safety-critical software
- High-confidence software within predictable cost and schedule
- High confidence for new types of software, such as for model-based autonomy and adaptive control
- Sustained engineering (for example, the ISS and the Space Shuttle)
- Security for ground and radio frequency networks

Several major programs span the agency's technical readiness level (TRL) scale, which runs from 1 to 9 (9 denotes a capability that has served on the space shuttle for 50 flights). High-TRL work has a strong process orientation, mid-TRL is work in transition to practice, and low-TRL work involves fundamental research. HCSS-related efforts include:

Computing, Information and Communications Technology (CICT) – (low- to mid-TRL) project aims to develop automated mathematical techniques for the software development process, yielding tools for cost-effective development of high confidence, highly reliable software systems for aerospace applications. Its goal is to develop technologies with enhanced capabilities to:

- Analytically verify the next generation of aerospace software:
  - Scalable software model checking
  - Automated program abstraction
  - State-space search algorithms
  - Formal method verification of integrated modular

avionics design

- Produce certifiable program synthesis for the following technologies:
  - Program generation through automated reasoning
  - Product-oriented certification methods
  - Automated tools that certify automatically synthesized code
- Develop adaptive, integrated software verification and monitoring technology, including:
  - Runtime monitors generated from requirements specifications
  - Automated behavioral verification
  - Machine learning to optimize exploration of potential behaviors
  - Automated generation of software fault recovery

These capabilities would then be applied to specific missions such as the ISS and the Mars Lander.

Highly Dependable Computing Platform Testbed – provides a modern software platform for real-time embedded systems. The approach (low- to mid-TRL) is to evaluate real-time Java to address in-flight software demands and use the Mission Data Systems (MDS) framework and software as a testbed. While NASA typically runs older hardware on the ISS and the Hubble telescope because that hardware is known to be hardened against radiation, it develops software on modern workstations and then ports that software to the older hardware. The real-time Java needs to have demonstrably lightweight CPU usage and provide the desired throughput and response. NASA needs to be sure that timing jitters do not surface and cause problems.

Mission Data Systems (MDS) – (mid-TRL) developing a reusable infrastructure for flight and ground software for the mission to Mars in 2009. In preparation for the launch, all needed technologies should be in place in 2005. MDS is integrating the best systems engineering and software engineering practices for autonomous control of physical systems. The program was developed for unmanned space science missions involving spacecraft, landers, rovers, and ground systems. It is broadly applicable to mobile and immobile robots that operate autonomously to achieve goals specified by humans. It is also architecturally suited for complex interactive systems where "everything affects everything."

As complexity grows, the line between specifying behavior and designing behavior is blurring. For each of the items in the following illustrative list, systems engineers need to know and want to specify the item, while software engineers want to design software that knows the item:

- How a system is put together (connections and other interactions)
- What functions each element performs (models of behavior)
- How system elements might fail (models of faulty behavior)
- What the environment is like and how it affects the system (more models)
- What the system must be able to do (scenarios and their objectives)
- What operating constraints the system must honor (flight rules, etc.)
- What resources the system must manage (power, data storage, etc.)

The MDS approach is through product line practice to exploit commonalities:

- Define a reference architecture to which missions and products conform
- Provide framework software to be used and adapted
- Define processes for systems engineering and software development

An example is state analysis for embedded systems. The Mars science lab now has some 10,000 state variables. The relationship between each pair (for example a disk drive's power and the heat it produces) is described and the software is designed to include rules on determining and controlling state. This effort helps systems engineers and software engineers use the same vocabularies.

Office of Safety and Mission Assurance Research Program – mid-TRL effort that encompasses the following:

- Software assurance practices for auto-generated code:
  - Evaluation of available artifacts from autocode processes
  - Verification of the code generator
- Software assurance practices for commercial off-the-shelf integration:
  - V&V of interface to COTS

– Validation of a COTS application for an intended purpose

- Software assurance practices for reused or heritage software:
  – Reuse or heritage factors that impact software risk
  – Appropriate level of software assurance for reused or heritage code
- Reliability of operating systems
- Tandem experiment to improve software assurance
- Independent V&V (IV&V):

IV&V is verification and validation performed by an organization that is technically, managerially, and financially independent. IV&V focuses on mission critical software, provides addition reviews and analyses, and provides in-depth evaluation of life cycle products that have the highest level of risk. Examples of IV&V activities include the following:

- Validation of design to meet system needs and requirements
- Traceability of safety-critical requirements
- Code analysis of mission-critical software components
- Design analysis of selected critical algorithms

Software Engineering Initiative (SEI) – high-TRL effort begun to respond to the growing complexity, size, and sophistication of software components (for example, the two Mars missions that landed in January 2004 involve 625,000 lines of source code). The goal of the SEI is to advance software engineering development, assurance, and management practices to meet NASA's science and technology objectives. Elements of this initiative include:

- Plans from each center to improve software process and products
- Use of the Carnegie Mellon University Software Engineering Institute's Capability Maturity Models (CMM) as benchmarks for assessments
- Infusion of the "best of the best" software engineering research and technology
- Software metrics to monitor the initiative's progress and to provide early warning of problems
- Effective guidelines, principles, and standards
- Enhanced knowledge and skills in software engineering through training, education, and information exchange
- Improved software acquisition capabilities

Software Assurance Program – (high TRL) seeks the following:

- Software risk mitigation
- Improved quality of software products while using risk mitigation techniques
- Project management insight into software development processes and products throughout the life cycle
- Early error detection, problem prevention, and risk identification and mitigation
- Improve the quality of future products and services

The level of software assurance needed is dependent on the software size, complexity, criticality, and level of risk. Software assurance covers practices for auto-generated code, COTS integration, and reused or heritage software. Software assurance work is performed in the following areas: standards; guidance; policy; contractor evaluation criteria; metrics; means to classify software across NASA; IV&V; research; benchmarking; and outreach.

Software assurance involves both software safety and software reliability, as follows:

- Software safety includes a systematic approach to identifying, analyzing, tracking, mitigating, and controlling software hazards and hazardous functions (data and commands) to ensure safer software operation within a system.
- Software reliability is the process of optimizing the software through emphasis on requiring and building in software error prevention, fault detection, isolation, recovery, tolerance, and/or transition to planned reduced functionality states. It also includes a process for measuring and analyzing defects in the software products during development activities in order to find and address possible problem areas within the software.

HCSS DARPA HCSS

Self-Regenerative Systems (SRS) – aims to develop a military exemplar system that shows it is possible to: provide 100 percent of critical functions at all times in spite of attacks; learn about one's own vulnerabilities to improve survivability over time; and regenerate service after attack. The result of SRS activities will be intrusion-tolerant systems that gracefully degrade and recover after an attack while maintaining some level of system performance instead of crashing. The development phase will involve self-regenerative systems that restore performance to full operational capability. SRS technical areas include the following:

- Biologically Inspired Diversity to reduce common software vulnerabilities to attack by providing different versions of software with different implementations and configurations
- Cognitive Immunity and Healing systems that incorporate biologically inspired response strategies and machine learning to identify and correct root causes of vulnerabilities
- Reasoning About Insider Threats to pre-empt insider attacks or detect system overrun by combining and correlating information across system layers, inferring user goals, and enabling effective anomaly detection
- Granular, Scalable Redundancy to survive massive attacks or extreme hostility by approach exploiting environment knowledge to scale or perform and develop probabilistic consistency protocols that will survive extremely hostile environments and provide "good enough" service

Security-Aware Systems.– goal is to minimize unavoidable cyber risk to military missions by having the system itself smoothly adapt to changing resources, building blocks, security requirements, mission goals, and threats. A security-aware system will reason about its own security attributes, capabilities, and the utility of its functions with respect to a mission context. It will dynamically adapt to provide desired levels of service while minimizing risk and providing coherent explanations of the relative safety of service level alternatives.

In FY 2005, work will continue on the following DARPA effort:

- *Self-Regenerative Systems (SRS)*

The following DARPA effort is new for FY 2005:

Security-Aware Critical Software (SACS) program – *will create a new generation of software that provides a comprehensive picture of security properties and current status, presenting this information at multiple levels of abstraction and formality. SACS will thus make security properties and status transparent to decision makers, which will increase the speed and confidence with which military systems can be securely and dynamically reconfigured, particularly under stressful conditions. SACS will enable construction of a security-aware system that can reason about its own security attributes and capabilities and the utility of its functions with respect to a mission context. The software will dynamically adapt to provide desired levels of service while minimizing risk and providing coherent explanations of the relative safety of service-level alternatives.*

HCSS NIST HCSS

Two divisions in the Information Technology Laboratory at NIST – the Software Diagnostics and Conformance Testing Division (SDCTD) and the Computer Security Division (CSD) – are the primary organizations involved in HCSS activities. The SDCTD mission is to develop software testing tools and methods that improve quality, conformance to standards, and correctness, and to work with industry to develop forward-looking standards. Five technical areas of SDCTD involve HCSS R&D:

Electronic Commerce – focuses on extensible markup language (XML), a universal interchange format including core technologies. More generalized than HTML and can be used for tagging data streams more precisely and extensively. World Wide Web Consortium (W3C) interoperability testing will be conducted to evaluate interoperability in both messaging and smart card services. NIST aims to develop and automate consistent, complete, and logical specifications and turn these into performance testing for eventual commercial use.

E-Health – developing Health Level Seven (HL-7) standards and conformance and a standards roadmap so that medical devices, hospital systems, and other health care service provider systems can talk to each other while protecting patient privacy. NIST is working with the Department of Veterans Affairs on access control, sign-on, and other procedures, acting as a trusted impartial "third party" among providers, researchers, manufacturers, and others to promote effective access controls.

Computer Forensics – working with the FBI and the National Institute of Justice to develop a National Software Reference Library (NSRL) and specifications and evaluations of computer forensics tools to use in efficiently analyzing seized property such as disk drives and verifying that rules of evidence are observed.

Pervasive Computing – addressing development of wireless service discovery protocols for wireless devices such as palm pilots to assure trustworthy interactions.

Test Method Research – fundamental work in object-oriented component testing and in automatically generating tests from formal specifications in a cost-effective manner.

FY 2004 new opportunities – conformance testing for medical devices and test suites for medical device communication standards; using the NSRL for data reduction, integrity management, and computer security applications; and investigating grid computing vulnerabilities to identify requirement for maintaining system robustness.

The mission of the CSD is to improve information systems' security by: raising awareness of IT risks, vulnerabilities, and protection requirements; researching, studying, and advising agencies of IT vulnerabilities and devising techniques for cost-effective security and privacy of sensitive Federal systems; developing standards, metrics, test and validation programs; and developing guidance to increase secure IT planning, implementation, management, and operation. CSD programs encompass the following:

Security Technologies – cryptographic standards, key management, public key infrastructure (PKI), identity management, protocols and e-government, and agency e-government support

Systems and Network Security – technical guidelines, checklists, smart cards, wireless/mobile, Intrusion Detection System (IDS), ICAT, IP Security Protocol (IPSec), authorization management, automated testing, and quantum cryptography

Management and Assistance Program – outreach, expert assistance, policy, and guidelines, and Information Security and Privacy Advisory Board (ISPAB)

Security Testing and Metrics – security control development, certification and accreditation, cryptographic module validation, laboratory accreditation, and the National Information Assurance Partnership (NIAP)

FY 2004 new opportunities – a Standard Reference Model (SRM) for source code security to develop a metric for automated tools to review security properties of software and a database of known security flaws from "buffer overflow" through "trap doors"; trust and confidence taxonomy (reliability, security, interoperability) or "-ilities" toolkit

NIST FY 2005 plans in HCSS-related R&D include:

- *Continue work in electronic commerce, e-health, computer forensics, test method research, security technologies, systems and network security, management and assistance, and security testing and metrics*
- *Possible new activity in high-confidence methods for voting and vote counting*

PARTICIPATING AGENCIES

HCSS

FAA

HCSS

FAA's Office of the Assistant Administrator for Information Services and CIO focuses on security, processes (enterprise architecture), and education issues. The Office must co-sponsor its research, have an FAA customer, and either have a short-term focus or collaborate with others on longer-term issues.

Over the past three years, FAA has evolved a systematic approach to defending the air traffic control system against cyber attack:

- Harden individual system and network elements
- Isolate elements to avoid "viral" spread
- Replicate elements to avoid service disruption

This strategy is difficult because of the size and complexity of the air-traffic-control system, the increased use of COTS products, and the safety-critical nature of the air-traffic control system. Significant challenges such as building trustworthy systems with untrustworthy components remain. FY 2004 AIO activities are:

- Rapid quarantine capability
- Wireless information systems security
- A Common Criteria test lab
- Integrity and confidentiality lab
- Estimating security costs
- A software reliability pilot
- Biometrics for single sign-on
- Data mining for vulnerabilities

HCSS

FDA

HCSS

FDA, through its Center for Devices and Radiological Health, with other agencies develops medical devices that require high-confidence, assured, safe software to deliver quality medical care. The FDA Office of Science and Technology leverages funds to work with other agencies. Research interests focus on formal methods of design in three areas:

- Safety and safety modeling
- Certification issues
- Forensic analysis

Specific research projects include:

- Life Support for Trauma and Transport (LSTAT), an intelligent litter platform with Walter Reed Army Medical Center (safety and safety modeling) • Proton beam therapy device (safety and safety modeling)
- Software for an infusion pump with a control loop, which led to an initiative to develop similar control loop software for a ventilator device (certification)
- Blood bank software regulation (certification)
- Radiation-treatment planning systems that employ reverse engineering of C programs to look for inconsistencies and errors in analysis of brain tumors (forensics)

HCSS

AFRL

HCSS

The Air Force Research Laboratory in Dayton, Ohio is working on developing certifiability requirements for autonomous aircraft that operate in civilian and military airspace.