Cyber Security and Information Assurance (CSIA)

NITRD Agencies: NSF, DARPA, OSD and DoD Service research organizations, NIH, NSA, NASA, NIST
Other Participants: DHS, DOT, FAA, FBI, IARPA, State, Treasury, TSWG

CSIA focuses on research and development to prevent, resist, detect, respond to, and/or recover from actions that compromise or threaten to compromise the availability, integrity, or confidentiality of computer- and network-based systems. These systems provide both the basic infrastructure and advanced communications in every sector of the economy, including critical infrastructures such as power grids, emergency communications systems, financial systems, and air-traffic-control networks. These systems also support national defense, national and homeland security, and other vital Federal missions, and themselves constitute critical elements of the IT infrastructure. Broad areas of concern include Internet and network security; confidentiality, availability, and integrity of information and computer-based systems; new approaches to achieving hardware and software security; testing and assessment of computer-based systems security; and reconstitution and recovery of computer-based systems and data.

President's 2009 Request

Strategic Priorities Underlying This Request
CSIA R&D includes both foundational and applied research across the broad range of technologies and capabilities needed to improve security, assurance, and trust in the computer-based systems and networks that support national defense, national and homeland security, economic competitiveness, and other national priorities. Key research areas include:

Near-term functional cyber security and information assurance: Improvements in operating systems, cryptography, and identity management that enable systems of national significance to function as intended in the face of cyber events; software protection, assured information sharing, and collaboration across multiple domains and security enclaves; indications and warnings for situational awareness and responses to full-spectrum, multi-layer cyber attack (e.g., detection, assessment, attribution, automated response); methods for assured operations in high-threat environments including rapid reconstitution

Longer-term infrastructure and scientific foundations: Policy-based security management infrastructure for processing, storage, and communication of sensitive information; security for emerging network technologies (e.g., mobile, wireless, pervasive computing); computational foundations of software engineering to develop high levels of assurance in next-generation information-intensive systems; empirical and analytical studies to measure and validate new concepts for a principled approach to building complex systems rapidly, securely, and affordably

Larger social issues: Privacy concerns of individuals; usability of technologies; public awareness of IT risks, vulnerabilities, and protection requirements, particularly for emerging technologies; cost-effective techniques for security and confidentiality of sensitive Federal systems; standards, metrics, tests, and validation programs to promote security in systems and services, educate consumers, and establish minimum security requirements for Federal systems; guidance on secure development, implementation, management, and operations; education of next-generation cyber security workforce

Highlights of Request

Team for Research in Ubiquitous Secure Technology (TRUST): Multi-university center with industrial partners to develop new science and technology that will transform the ability of organizations (software vendors, operators, local and Federal agencies) to design, build, operate trustworthy information systems for critical infrastructures; allied centers in specific topics (ACCURATE, CCIED, TCIP, SAFE) – NSF

Software protection: Develop novel assurance technologies (e.g., automated function extraction, kernel-mode protection, anti-forensics) for critical software such as weapons codes; enable software to detect and react to unauthorized use (autonomic protections); software provenance analysis; hardware and software tamper-proofing methods – DARPA, OSD, AFRL, ONR, NSA

Secure software engineering: Develop theoretical foundations and precise standards, technologies, automation methods for engineering software security and survivability; software vulnerability, cost-benefit analysis tools (e.g., OSD's QuERIES); security practices for early phases of systems development lifecycle; ontology of security properties; formal methods for validation, verification of composable systems; lightweight analysis; online program disassembly – NSF, OSD, AFRL, NIST

Security management infrastructure: Develop policy-based access control systems; principles, frameworks, models, methods for identity, authentication, and privilege management in dynamic environments; management tools (threat analysis, attack- and risk-based decision models; survivability analysis

framework; automated and real-time diagnostics for system security-policy flaws, configuration anomalies, vulnerabilities; Resiliency Engineering Framework for assessing organizational security-management capabilities) – NSF, DARPA, OSD, AFRL, ARO, NSA, NIST

Assured information sharing: DoD-wide priority to enhance technologies and tools to secure communications and data sharing across multiple, heterogeneous networks, platforms, security levels, and secure enclaves (e.g., AFRL's Assured, Load-Balancing Enterprise); high-assurance, programmable, certifiable guard; secure virtualization platforms (SVPs) protecting systems from software-based attacks; demonstrate secure collaboration through cyber sensing station – OSD and DoD Service research organizations, NSA

Network defense: Technologies and tools for situational awareness, threat anticipation, characterization, and avoidance, attack warning, intrusion protection and detection, and rapid response (containment, repair, self-regeneration to operational state); behavior-based network monitoring and active defense; defense against large-scale attacks (e.g., DDoS, worms, botnets, spyware); prototype cyber operations center; security of emerging net-centric systems of systems and strategic computing resources (e.g., NASA perimeter protection effort) – NSF, DARPA, OSD, AFRL, ARL, ARO, ONR, NSA, NASA, NIST

Cryptography: Cryptographic algorithms and engineering; identity-based encryption; provable security; key management; lightweight cryptographic systems; conditional and revocable anonymity; improved hash functions; photonics, novel materials, classical and quantum cryptographic methods and standards – NSF, DARPA, OSD, ONR, NSA, NIST

Cryptographic Hash Competition: Worldwide competition in which candidate algorithms are submitted for selection as a NIST Federal Information Processing Standard (FIPS) – NIST

Privacy: Privacy-preserving technologies and methods; location privacy – NSF, NSA, NIST

Wireless and sensor networks: Assured access, jamming-resistant communications (advanced antennas, software-defined radio technology, RF watermarking); RFID counterfeit detection; analytical and simulation techniques, standards to characterize mobility protocols; security technologies, pervasive computing – NSF, DARPA, OSD, AFRL, ARO, NSA, NIST

Standards, testing, and metrics: Quantitative risk-analysis methods and tools; quantitative methods and tools to support cryptographic conformance determination and validation; models and standards for protection, sharing of sensitive information; standards and tests to assess, validate system security; trusted computing base; development of trustworthy protocols, applications (BGP, IPv6, SIP, DNS); leadership in national and international standards bodies – NIST, NSF, OSD, ARL

Planning and Coordination Supporting Request

Roadmapping process: Use inputs solicited from Federal, industry, and academic representatives to inform planning activities; in partnership with these groups, develop an R&D roadmap associated with priorities and gaps identified in the *Federal Plan for CSIA R&D* – CSIA IWG

Co-funding: NSF TCIP Center – DHS, DOE/OE; biometrics R&D – NSF, NIST, DHS; secure core, formal verification, security-related software errors R&D – NSF, DARPA

Research data: Collaboration in research data confidentiality and usability – NSF, NIH

Information Security Automation Program: Multiagency collaboration to address deficiencies in how vulnerabilities (software flaws and misconfigurations) are described, checked, remediated, and mapped to compliance policies – NIST, OSD, NSA, DISA

Computer security architecture: Planning meetings for possible multiagency activities – NSF, DARPA, OSD and DoD Service research organizations, NSA, CIA, DNI

Interagency cooperation: Discussions on secure and resilient recovery mitigation of systems against insider attacks, possible R&D co-sponsorship – NSF, Treasury; deployment and testing of prototype security technologies – OSD, DOE/NNSA; intrusion detection/monitoring, intrusion-tolerant systems – DARPA, AFRL, NSA; proposal reviews – multiple CSIA agencies

Workshops: Security and privacy for sensor networks and embedded systems – NSF, AFRL, ARO; privacy and data confidentiality – NSF, vendors; Cryptographic Hash Competition – NIST, Federal agencies, academia, vendors; Federal Desktop Core Configuration (FDCC) – NIST, Federal agencies, vendors; Security Content Automation Protocol (SCAP) – NIST, Federal agencies, vendors

International collaboration: EU workshop on experimental evaluation and collaborative defenses; supplemental travel grants for Japanese and NSF researchers for collaborative research – NSF, Japan, EU; ministerial-level efforts to promote Internet privacy and IP protection – NSF, OECD; TTCP Information Assurance and Defensive Information Warfare Panel (Australia, Canada, New Zealand, UK and U.S.) - DoD; IETF security standards panels – CSIA agencies

Testbeds and methods for experimentation and evaluation: Continued joint development of research testbeds including DETER, ORBIT; repository of anonymized sharable test data based on actual

events/behaviors; open- source software and wide distribution of benchmark results; open-source communication simulation models – NSF, OSD, NIST, DHS

INFOSEC Research Council: Provides a forum for coordination of ongoing R&D and develops long-term research agendas through the *Hard Problem List* – Multiple agencies

Additional 2008 and 2009 Activities by Agency

NSF: Continue investments in Cyber Trust; support for cyber security research including formal methods (access control rules analysis, analysis of policy, verification of composable systems, improved trust functions); formal models (access control, artificial diversity and obfuscation, deception); applications (critical infrastructures, health records, voice over IP, geospatial databases, sensor networks, federated systems); hardware enhancements for security (virtualization, encryption of data in memory, high performance IDS, TPM); security enhancements for research cyberinfrastructure; emphasis on usability, privacy, and theoretical foundations

DARPA: Trusted, Uncompromised Semiconductor Technology (TrUST) program R&D to advance science and technology for ensuring that integrated circuits (IC) can be trusted regardless of origin and fabrication process

OSD: Methods to analyze, synthesize network flow for situational awareness across organizations; application-centric protections against nation-class and insider threats; automated, scalable, adaptable, sustainable, protections; high assurance secure virtual platforms; tools for malware detection, analysis, and removal; protection of high-speed networks and supercomputer centers

AFRL: Prototype cyber operations center; cyber craft; cyber attack detection/traceback/attribution (with IARPA, Firestarter); insider threat indicators; digital data embedding including steganography and watermarking

ARO/ARL/CERDEC: Collaborative technology alliance in communications and networks; intrusion detection for MANETs; highly efficient security services and infrastructure

ONR: Data fusion and data mining; maritime domain awareness; surveillance

NSA: Centers of Academic Excellence (recognition for universities doing IA R&D); Scholarship for Service; security for mobile devices in hostile environments; high-speed cryptography

NASA: Perimeter controller/enforcer for dynamic port-access control for network-intensive applications; two-factor authentication for remote access to HEC systems; secure unattended proxy (SUP) for automated file transfers

NIST: Configurable access control mechanism (supported by DHS); National Vulnerability Database (funded by DHS); automated combinatorial testing; technical security guidance documents for Federal agencies; methods for detecting, identifying botnets; cryptographic standards; planning for cryptographic hash competition; mathematical foundations of measurement science for information systems

TSWG: SCADA Cyber Attack Alert Tool to alert operators to the existence, nature, and extent of cyber attacks through reports based on a standard set of attack definitions against geospatially distributed, resource-limited, and time-critical systems