Cyber Security and Information Assurance (CSIA)

NITRD Agencies: NSF, OSD and DoD Service research organizations, NIH, DARPA, NSA, NASA, NIST

Other Participants: DHS, DOT, DTO, FAA, FBI, 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.

NITRD Program: Coordination Activities Highlights
In 2006, the first full calendar year in which the CSIA Program Component Area (PCA) and the CSIA Interagency Working Group (IWG) were formally part of the NITRD Program, the CSIA agencies completed the *Federal Plan for Cyber Security and Information Assurance Research and Development* (April 2006) and began planning for follow-on activities. In key recommendations, the report called for development of a sustained, coordinated multiagency effort to address CSIA R&D, and proposed that the Federal government initiate a collaborative activity in partnership with industry and academia to develop a roadmap for Federal CSIA R&D.

As the first step in the roadmapping activity, the CSIA IWG in November 2006 broadly disseminated a Call for White Papers that invited interested stakeholders to address topics either related to CSIA R&D technical areas or to roadmapping processes and structure. The papers, which enable stakeholders to provide input that can help shape the future research and development agenda for CSIA technologies in the United States, are supporting the IWG's planning for workshops and other roadmapping-related activities in FY 2007-2008.

President's 2008 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:

Functional cyber security and information assurance: R&D to secure and protect large-scale and mission-critical information systems and networks, including approaches, methods, and tools for attack protection, prevention, detection, preemption, warning, mitigation, recovery, and forensics; situational awareness; access control and privilege and trust management; software protection

Infrastructure and domain-specific security: DNSSEC deployment; secure routing protocols; secure process control systems for critical infrastructures; wireless security, assured access; security for emerging networks, supercomputers, and heterogeneous traffic

Cyber security and information assurance assessment: Techniques and tools for software vulnerability and malicious code detection and analysis; system security and survivability standards and benchmarking; security and assurance standards, metrics, tests, and automated verification and validation methods

Scientific foundations: R&D in hardware and firmware security; secure operating systems; self-regenerating systems; trustable end devices; security policy management methods; cryptography, multilevel security; secure software engineering and lifecycle management; incorruptible data, code, executables; high-assurance, "secure by construction" code development methods and assured information sharing

Highlights of Request

Team for Research in Ubiquitous Secure Technology (TRUST): Multiuniversity 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 and operate trustworthy information systems for critical infrastructures – NSF

Software protection: Develop high-assurance software protection and secure software engineering; implement out-of-band defense strategies, tamper-proof hardware, secure-application-launch protection for trust in end nodes; ubiquitous and seamless Secure Development Environment supporting the lifecycle of critical application software and data – OSD, AFRL, ARL/ARO/CERDEC, ONR/NRL, NSA, NSF, TSWG

Trusting the edge: Develop and validate technologies, techniques, and tools to provide distributed trust and assurance for the Global Information Grid (GIG) and mission-critical net-centric domains such as high-confidence airborne networking (by enabling an edge device to protect itself in a hostile environment and by creating the ability to monitor and assess its integrity) – OSD, AFRL, ARL/ARO/CERDEC, ONR/NRL, DARPA, NSA

Cognitive systems: Leverage technologies in learning, reasoning, deliberation, and reflection to develop systems that can maintain and improve critical functionality despite repeated attacks or errors – DARPA

Security management for critical infrastructures: Fundamental and applied R&D to advance and harden against attacks and system failures, especially for the automated computing systems and devices that control power grids, industrial processes, air-traffic-control systems, financial networks, wireless networks (cellular telephones) and other critical infrastructures – NSF, NSA, NIST, DHS, TSWG

Measurement science and technologies: Identify and address vulnerabilities in real time, assess effectiveness of security controls, and mitigate attacks; security metrics, test and validation – NSF, NSA, NIST, DHS, FBI

Situational awareness and response: Security event visualization and management and reconstitution of network assets and services based on cyber attack or physical fault; seamless, integrated situational awareness, rapid automated protection response, and behavior-based network monitoring capabilities – NSF, OSD, AFRL, ARL/ARO/CERDEC, NSA, DHS

Assured information sharing: Virtual private network, secure collaboration technologies; secure routing protocols, key management, identity management technologies; high-assurance, programmable guard; hardware enhancements; models and standards for protecting and sharing sensitive information and thwarting identity theft – NSF, OSD, AFRL, ONR/NRL, NSA, NIST, DHS

Testbeds: Cyber Defense Technology Experimental Research (DETER) cyber security testbed; security plan for GENI; infrastructure for R&D – NSF, NIST, ARL/ARO/CERDEC, DHS

Wireless: Advanced antennas for WLANs; insider threat detection, response**;** software-assisted (cognitive) radio technology**;** RF watermarking – NSF, OSD, AFRL, ARL/ARO/CERDEC, ONR/NRL, DARPA, NSA, NIST, DHS

Planning and Coordination Supporting Request

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

Network security issues: Collaborative activities in vulnerability assessment, intrusion detection and monitoring, fault-tolerant systems, proactive protection and mitigation strategies leading to a broadly applicable, deployable trustworthy platform – AFRL, ARL/ARO/CERDEC, DARPA, DHS, DTO, NSA, NSF, ONR/NRL, OSD

Software protection technologies: Develop and deploy new software-protection technologies in high-performance computing environments; gauge effectiveness through red-teaming activity – NASA, NSA, OSD

Grand challenge in security: Planning for possible co-sponsored competition to develop a secure system that will withstand attack – DARPA, DTO, NSF

Research data confidentiality and usability: Planning for joint proposal solicitation – NIH, NSF

Grants and proposals: Collaborate/coordinate on solicitations, reviews, evaluations, and funding – DARPA, DHS, DTO, NIST, NSA, NSF

Security metrics and measurement: Joint planning for a workshop – NIST, NSF

International coordination: U.S./UK technology alliance in network and information sciences – ARL; U.S./UK cooperative science and technology agreement, U.S./Canada Public Safety Technical Program – DHS; research collaborations with Japan and EU on security for control systems and other security-related topics – NSF

National Plan for Research and Development in Support of Critical Infrastructure Protection: Provide input to the NSTC Subcommittee on Infrastructure on cyber aspects of critical infrastructure protection – CSIA IWG

INFOSEC Research Council: Provides a forum for near-term operational R&D focus and proposes a long-term research agenda through the *Hard Problems List* – Multiple agencies

Additional 2007 and 2008 Activities by Agency

NSF: Industry/university cooperative research centers in information protection, security-critical applications, and experimental research in computer systems; ongoing awards in cryptography, formal methods, large-scale attack defense, preserving privacy in data mining, formal models; intrusion detection and response, hardware enhancements (virtualization, data encryption in memory, high-performance intrusion detection systems); future threats; education programs to prepare future generations of cyber security professionals

OSD: Security management infrastructure (techniques and tools for vulnerability analysis and risk assessment, benchmarking framework for improving operational security, virtual training environment); quantitative risk analysis methods; cyber forensics; secure coding techniques; innovative analysis techniques using DoD flow data; security technologies and tools for high-data-rate networks and supercomputing centers; participation in the Internet Engineering Task Force (IETF) security groups to develop standard representations and corresponding reference implementations of security-relevant data; SBIRs in topics to support GIG security

AFRL: Defensive cybercraft; network and system recovery and repair (with DARPA); predictable/customizable end-to-end QoS under degraded network conditions; large intrusion detection data analysis techniques; cyber attack detection/traceback/attribution (with DTO); digital data embedding; biometrics liveness

ARL/ARO/CERDEC: Secure, trustworthy information delivery in mobile tactical systems (including sensor networks); high-confidence software; self-healing survivable information system theory, modeling, and development; MURIs in high-speed wide-area-network intrusion detection, response, and analysis; distributed immune systems for wireless network information assurance; international technology alliance with U.K.

ONR/NRL: High-integrity multilevel security hypervisor providing secure foundation for server platforms; theories, techniques, and tools for developing security software; algorithms, methods for secure-by-construction development; MURI in adaptive trust management for service-oriented architecture; safe execution environments; protocol analysis; detection, exploitation of information in text, images, speech; voice biometrics

DARPA: Intrusion-tolerant information assurance technologies for current and emerging capabilities in mission-critical, command and control, intelligence, sensor, wireless, and mobile systems to provide survivable, trusted network-centric systems and cost-effective information protection solutions for DoD

NSA: Technologies for safe computing platform leveraging COTS hardware, virtualization, measurement, and attestation; intelligent, secure, flexible, self-protecting global infrastructure that provisions and monitors integrity of information assurance products and services through privilege management capability for dynamic (mobile) policy environments; cryptographic algorithms and engineering for faster networks; behavior-based network monitoring and active response capabilities; making information available to diverse users, but separable by classification, content, and intended use

NASA: Technologies and tools to enable seamless, secure network-intensive distributed high-end applications with strong perimeter protection system; approaches include secure unattended proxy (SUP) and perimeter controller/enforcer

NIST: Identity management; Federal information security standards and guidelines; cryptographic standards, forensics; authentication; vulnerability, database and reference data; access control and attribute management; RFID; state and local outreach; secure OS and application configuration specifications; personal identity verification compliance test generation; authentication effectiveness metrics; technology-specific security guideline development; automated combinatorial testing

DHS: Protected Repository for the Defense of Infrastructure Against Cyber Threats (PREDICT), library of network datasets for use by security developers; R&D in emerging threats (e.g., virtual machine environment, next-generation crimeware, botnet command and control); SBIRs; next-generation technologies (vulnerability prevention, discovery, and remediation; network attack forensics; technologies to defend against identity theft)

TSWG: Published a study of available software tools for critical infrastructure interdependency modeling; deployed Systems Administrator Simulation Trainer (SAST) with USMC; successfully tested a secure means of data communications between 10K commercial aircraft and air-traffic controllers (S-ACARS)