About the National Science and Technology Council

The National Science and Technology Council (NSTC) was established by Executive Order on November 23, 1993. This Cabinet-level Council is the principal means for the President to coordinate science and technology across the diverse parts of the Federal research and

National Science and Technology Council

Federal Plan

for

CH9 423.2465 Tm-0.0002 TcYBEOR

page intentionally left blank

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF SCIENCE AND TECHNOLOGY POLICY
WASHINGTON, D.C. 20502

improving cyber security and information assurance. However, these subjects are outside the scope of the Plan, which addresses only the role of Federal R&D.

Likewise, the Plan is not a budget document and thus does not include current or proposed agency spending levels for cyber security and information assurance R&D. Agencies determine their

Findings and Recommendations

Strategic interagency R&D is needed to strengthen the cyber security and information assurance of the Nation's IT infrastructure. Planning and conducting such R&D wil7ionquire concerted Federal activities on several fronts as well as collaboration with the private sector. The specifics of the strategy proposed in this Plan are articulated in a set of findings and recommendations. Presented in greater detail in the report, these findings and recommendations are summarized as follows:

1. Target Federal R&D investments to strategic

9. Institute more effective coordination with the private sector

The Federal government should review private-sector cyber security ane coordinnformwith tassuranc -1.1T*ate acoocesoordicountermeasuresoto help idoulify-1.1T*at

The Federal Plan in Summary

In this Plan, the terms *cyber security* and *information assurance* refer to measures for protecting computer systems, networks, and information from disruption or unauthorized

In August 2005, the group was rechartered to report jointly to the NSTC Subcommittee on Networking and Information Technology Research and Development (NITRD) as well as to the Subcommittee on Infrastructure, in order to improve the integration of CSIA R&D efforts with other NITRD program component areas and coordination activities (see Appendix B). In conjunction with the rechartering, the group was renamed the Cyber Security and Information Assurance (CSIA) IWG to better characterize the scope of the IWG's activities and to reflect the fact that cyber security and information assurance are essential to critical information infrastructure protection but also have a broader impact.

The IWG assumed the responsibility for gatherorkiinformation about agencies' cyber security and information assurance R&D programmatic as activities achallenges,ies afor developing an interagency Federal planafor cyber security and information assurance R&D. This document, which representtie collaborative effort of the CSIA IWG agencies, settiforth a baseline framework for coordinated, multi-agency as activitithat continue to develop and implement the Federal Plan.

The framework is deroved from a CSIA IWG analysitithat identified and prioritized cyber security and information assurance R&D needs asross Federal agencies. The framework also includitiextensive documentation of the current state of the art and major technical challenges asross a spectrum of R&D areas of importance in the development of cyber security and information assurance technologies.

The *Federal Planafor Cyber Security and Information Assurance Research and Development* also servities a foundational documentafor the *National Critical Infrastructure Protection Research and Development Plan* (NCIP R&D Plan), which is required by Homeland Security Presidential Directive (HSPD) 7. Developed by the NSTC's Subcommittee on Infrastructure, this latter plan focusition R&D needs in support of protecting the Nation's critical infrastructures. The CSIA Plan focusition R&D to help meet IT needs outlined in the NCIP Plan, supporting CSIA elements of key NCIP strategic goals, including a national common operating picture, a secure national communication network,ies aa resilient, self-healing, self-diagnosorkiinfrastructure.

The CSIA IWG has begun to implement the

the opportunity to support or directly engage in

Threat and Vulnerability Trends

In addition to the exploitation of Internet vulnerabilities, adversaries seeking to gather sensitive information, commit crimes, or attack critical U.S. infrastructures can employ other means, such as:

Insiders

The key to malicious or hostile activities in cyberspace is access to networked systems and information. Facilitating this access through the use of insiders can greatly reduce the technological sophisinfotion necessary to mount an attack, because autheninfoted and authorized insiders may be able to circumveni barriers to external access, or may have legitimate access rights and privileges that would be denied to unauthorized users. So while obtaining network access via hacking provides one poteninal path for malicious activity, insider

particularly by terrorists but also by foreign intelligence services; espionage against sensitive but

Recent Calls for Cyber Security and Information Assurance R&D

In addition to the historic Federal role in supporting long-term R&D, significant drivers for Federal cyber security and information assurance R&D arise from current national circumstances and Federal priorities. These drivers are identified in a number of Federal documents.

OSTP/OMB Memorandum on FY 2007 Administration R&D Budget Priorities

In a July 2005 memorandum entitled “Administration R&D Budget Priorities for FY

The-1.eral guidance memo cites cyber secdoc.elt4a-1.2 -1.1667 TD(tancum one of three pryss at areum in on)T$3-

- Mitigation and recovery methodologies
- Cyber forensics
- Modeling and testbeds for new technologies
- Metrics, benchmarks, and best practices
- Non-technology issues that can compromise cyber security

The National Strategy to Secure Cyberspace

The February 2003 *National Strategy to Secure Cyberspace* calls for Federal R&D leadership in certain circumstances, such as to address an

3. Develop and accelerate the deployment of new communication protocols that better assure the security of information transmitted over networks.

4. Support the establishment of experimental environments such as testbeds that allow government, academic, and industry researchers to conduct a broad range of cyber security and information assurance development and assessment activities.

5. Provide a foundation for the long-term goal of economically informed, risk-based cyber security and information assurance decision making.

6. Provide novel and next-generation secure IT concepts and architectures through long-term research.

7. Facilitate technology transition and diffusion of Federally funded R&D results into commercial

Investment Analysis

In the third step of the baseline development

– automated attack detection, warning, and response – was among the top-funded priorities although it was not rated as a top technical priority.

The following topics are ranked as interagency technical priorities but are not among the top funding priorities: large-scale cyber situational awareness; secure process control systems; security of converged networks and heterogeneous traffic; detection of vulnerabilities and malicious code; IT system modeling, simulation, and visualization;

Cyber Security and Information

- Although privacy was not camo m2out as a single technicam area among the PITAC priorities, it was mention m2as a subtopic within three of its priorities (authentication technologies, holistic system security, and non-technology issues that can compromise cyber security). In contrast, the IRC did focus specificamly on privacy, having identifi m2security with privacy as on of the IRC's hard problems. Similarly, privacy was identifi m2as on of the CSIA IWG's top technicam priorities.

- Other PITAC research priorities and IRC hard problems not identifi m2by the CSIA IWG as interagency R&D priorities are clearly mission-related priorities that are receiving emphasis within individuam agencies. For example, the DHS focus on infrastructure protection is represented in a program aim m2at2securing fundamentam Internet communication protocols, including the Domain Name System and routing protocols – squarely within the scop of the PITAC priority of secure fundamentam protocols. Both DoD and DHS are funding work in recovery and reconstitution, which corresponds to the PITAC research priority of mitigation and recovery methodologies. DoD, DHS, and intelligence community work inD,

The technology trends outlined in this report make clear that the U.S. faces a long-term engagement with a new type of challenge to its security and economic stability. Cyber threats are asymmetrical, surreptitious, global, and constantly evolving. Moreover, the pervasive interconnectivity of the IT infrastructure on which

R&D in information technologies, where overall advances require gains in many scientific disciplines and component technologies.

Recommendation: Agencies should consider cyber security and information assurance R&D policy guidance (e.g., the joint memorandum from OMB and OSTP [discussed on page 13] that identifies cyber security as an interagency R&D priority) as they address their mission-related R&D. Agencies should also be aware of the interagency cyber security and information assurance R&D priorities identified in this report, and should give appropriate weight to these areas in budget formulation and technical program planning.

Recommendation: To achieve the greatest possible benefit from investments throughout the Federal government, cyber security and information assurance R&D should have high priority for individual agencies as well as for coordinated interagency efforts.

4. Support sustained interagency coordination and collaboration on cyber security and information assurance R&D

Finding: Cooperative interagency activities through the CSIA IWG enabled the development of this Plan. Sustained coordination and collaboration among agencies will be required to accomplish the goals identified in the Plan.
Ongoing coordination ctifc0.0001sSuhi6q cobentsshaill government, cyber security and informationasinterag required r

The IT infrastructure of the United States today is essential to the functioning of government, private enterprise, and civil society, including its critical systems for water, energy, transportation, and public safety. Federal leadership is both warranted and needed to encourage development of long-term goals and technical strategies for improving the overall security of this vital national interest.

The need for Federal leadership is underscored

Part II:

on
Cyber Security and Information Assurance R&D

1.2 Access Control and Privilege Management

Definition

Access control and privilege management begin with the administrative and mechanical process of defining, enabling, and limiting the operations that users can perform on specific system resources. The permission or limitation of operations is based on the business rules or access policies of the organization.

Access control policies are enforced through a mechanism consisting of a fixed system of functions and a collection of access control data reflecting the configuration of the mechanism. Together, these map

Therefore, a key research goal is to develop ways to
practicoalapplicoticon.5

efforts that are focused on understanding large volumes of low-level sensor data. Methods are needed to model and present to decision makers multiple, possibly competing, scenarios and hypotheses of unfolding potential attacks, in some cases with sufficient warning to preempt these attacks if possible, or at least minimize damage and support rapid, effective response and restoration.

Generation of situational awareness and understanding must be based on fusion of a broad

ability to provide an unalterable accounting of document access and dissemination – constitute a major Federal capability gap, given the sensitivity of many types of Federal information and the increasing demands for information sharing. The intelligence and DoD communities, which routinely handle many levels of dataable aocument sensitivity, have particularly acute concerns in this area. Document controlable integrity must be applied to the entire content in digital products, the potential for covert

The goal of traceback capabilities is to determine the

DNS registries) can often trace a path back to a host Internet service provider (ISP). Router netflow (a

The R&D topics in this category are focused on

designed and standardized. Difficulties arise from the attributes and assumptions of routing systems

- Secure self-organizing networks – classes of routing technologies that support wireless ad hoc and sensor networks as well as large-scale, peer-to-peer,

National testbed and testing program: Development of test methods based on test and evaluation criteria can form the basis for security evaluations of PCSs by

The R&D topics in this category focus on specialized

unauthorized scanning of tags, tracking of individuals or assets, or spoofing.

Research is needed on end-to-end security for the complete RFID life cycle since the privacy and security issues raised by RFID technologies are present from the manufacturing stage until the tag is destroyed. These issues are associated not only with the tags themselves but also with the readers and database management systems that store and process RFID information. Industry and government need to work together to develop technologies and policies to securely use RFID while maintaining confidentiality of sensitive data,rtai 2 ree managive daav’vacy and,T*(of saddnt sanagread to)sindilaw-toatict sys,

subscription-based priority service through

system, application type, and programming language). The results should be detailed enough that processes and tools can be designed to specifically counter the most common vulnerabilities, and that education efforts can be used to target the most common problems. Some rudimentary high-level statistics are available (e.g., statistics on buffer overflows or race conditions), but these statistics are not detailed enough to shed light on which processes or tools can

developing or using cyber security standards. Strategies are needed to encourage earlier buy-in to the process by all stakeholders.

Compliance testing helps assure that a product meets a cyber security standard and also helps isolate and correct security problems before the product enters the marketplace. Expeditious, cost-effective, and detailed technical test methods need to be developed for each component of an IT system. R&D that couples standards development with the creation of

The primary capability gap is at the very beginning of the software cycle, in the requirements, specifications, and top-level design phases. Current tools do not provide the precision and functionality to capture specifications in sophisticated modeling languages. Such languages could be used to generate measures of system complexity and completeness, identify design inconsistencies and ambiguities, minimize the likelihood of security vulnerabilities in an artifact that has been built to specification, and generate code and automated tests. The development of computotional tools to support the requirements analysis and design phases of system development would be an improvement over what has traditionally been a manual process.

Gaps also exist during the software implementotion phase. Avooi1.2a5roris and vulnerabilities in the

phase,s dies no kel mirate thenetedfor lratrd tesi1.n

aremaode anndrtaiols(areaddeds. tesi1.e and)TjT*(sasesement at theunite annsub system-level(aremoure)TjT*effenctvte t anv
senetetedfor post- development security analyiessunhn

iformcatio abouts design itmen. SSuchhas(system an)TjT* also(incrpoerate andent aceo exisi1.t tools tha s an)TjT*for know

arenetetef
phases of software developmen. Iin the
sdewi0oie4300tewelcte 2develops sunhen. Iin thbugabbetrate thenet.025 Tw(Tris wi0Current tools dohig2.0.* fy anar h or aA

State of the Art

In the business community, risk-based decision making methods have traditionally focused on risks of understand possible outcomes of their decisions and assess trade-offs between alternative actions.

Such understanding is of particular concern to critical infrastructure sectors that rely heavily on IT systems to operate, such as the banking and finance sector. Linking developing infrastructure interdependency consequence models with IT system operations and security models provides an opportunity to manage the risks from cyber and physical threats in a holistic way within and across critical infrastructures.

State of the Art

The general principles of control theory and control systems are relatively well understood. In addition, the physical and virtual commodity flows that IT systems control are generally well understood at an industry or company level. However, failures and consequences are often situation-dependent, and neither the interdependencies between the infrastructures nor the relationship between failures in

understood. Understanding these potential impacts requio

The topics in this category focus on fundamental technological elements that serve as building blocks for

S T
c
o
e
a
b
S
e
o
i
c
p

S S
i
d
l
c
l
c
d
t
a

economies of scale, and gain centralized control over legacy software applications that may have been developed in isolation. However, this business strategy carries risks. Legacy systems may not be fully integrated because of unresolved conflicts among security policies and organizational responsibilities, and thus may present vulnerable targets for attack.

Capability Gaps

Organizations and their operations will be hampered without the necessary security and security policies for accessing IT systems, networks, and information. Each organization must determine what constitutes

organization-wide IT infrastructure. Unfortunately, no ready-made solutions yet exist. The major gaps in the technical foundations for improved security regimes include the need for a rigorous semantic basis for policy specification languages and the need for assured consistency and acceptability of security policies between organizations.

5.5 Information Provenance

Definition

and digital rights management need to be integrated

a large amount of computation or is equivalent to

support a strong security policy. However, much of today's security is based on application-level user functionality and often does not use security mechanisms present in an OS. For example, a system can enforce strong network separation but may continue passing sensitive data if transfer policy enforcement is weak. A trusted OS can be the foundation for building a secure system, but an overall system design also needs to integrate strong security policies across all components of the system.

Validation and verification: A secure system needs an effective security policy, according to which information flow and system behavior are governed.

operations and maintenance, and sunset or disposition. During the initiation phase, the confidentiality, integrity, and availability objectives are specified. Assets that need to be protected are specified and a preliminary risk assessment is phdo aTD(dispositionsystemrdnitiation pmple the, the)minars

preclude such abuses. Resiliency and real-time fault-tolerance are crosscutting requirements in many mission- and safety-critical systems. Both these requirements as well as security requirements need to be effectively ahn50.4684

human virus propagation mechanism analogies. These emerging capabilities need to be integrated into new models of system complexity and security applications in large-scale enterprises.

Enterprise situational awareness: An accurate, real-time view of policy, enforcement, and exceptions is necessary for administration of networked systems of any size, and the larger the organization, the more difficult the problem. Situational awareness of the application of enterprise policy helps ensure that

Today, methods for protecting against or mitigating these kinds of attacks are not universally effective. However, because such attacks generally employ known techniques, the current statends the art in prevention and mitigation, which includes the emergencends self-healing networks and systems, is narrowing the gap. Several Federally funded networking and cyber security testbeds are aiding how an IT component works under both normal and atypical conditions. Simulation and visualization are used to determine how the systems behave over time and under a variety of conditions, and to convey that information to humans. Few components of IT systems are static – the systems are constantly being modified and upgraded – so the models themselves must be dynamic.

Imporre sstanT*h61980 -1.0001 Tcw(tic thc5 TT*flexibled umans. Few cper)Tjthe normal and

network traffic types and protocols; modeling of various classes of distributed cyber attacks; the lack of universally accepted topology, traffic, and protocol data associated with the Internet; and software integration of analytical and visualization tools.

6.5 Red Teaming

The topics in this category focus on methods, technologies, and architectures that will enable the creation of new generations of IT infrastructure components and systems that are designed and built to be inherently more secure than those in use today. The topics in this category are:

- Trusted computing base architectures

systems and middleware technologies that enable generally focus on addressing accidental faults and errors, intrusion-tolerant systems address intentional faults caused by a malos 2bs adversary. Autonomic computing uses automated management techniques to install software and patches, or to otherwise respond or adapt to changes in the computing environment such as failure-induced outages, changes in load characteristics, and addition of server capacity. Autonomic computing systems may not effectively respond to failures or changes in operating conditions due to malos 2bs attacks without being deliberately designed to do so.

Capability Gaps

Today, human operators decide how to protect systems from inadvertent cascading failures and malos 2bs attacks, which can occur even when some classes of cyber security tools are in place. Autonomic systems facilitate self-protection by: 1) monitoring systems and automatically improving system defenses (i.e., improving protective measures, configurations of IT, and cyber security systems); 2) using sensor reports to antos pate problems before they occur or identify them as they occur, and taking steps to avoid them or reduce their consequences; and 3) identifying emerging problems arising from failures or attacks that are not corrected by self-healong measures, and respondong to mitigate their impact. For example, an autonomic security system might provide automated security patch identification and deployment, or might automatically correlate security information across an enterprise to facilitate management of distributed protective measures.

Autonomic system technologies are needed to better protect systems and continually improve reliability,n0 792.03 612 -792 rees autngesprotect, imasures, contoy dinetworkautn

t i r u c e s e r

to centralized servers and distributed publish-and-subscribe settings, can include reasoning about the insider threat to preempt insider attacks; detecting system overrun by inferring user goals and intent; enabling anomaly detection; and combining and correlating information such as from system layers and direct user challenges.

Research is also needed on extended and refined end-to-end QoS models. Such models must provide a quantitative basis for efficient and effective resource management for adaptive, autonomic systems, enabling them to respond to changes due to overload, component failure, malicious attacks, evolving operationaTaang systnefined en0oeems,

Topics in this R&D category address the impacts of cyber security on people, organizations, and society, and the implications of cyber security for law, policy, and social systems. Topics in this category are:

- Trust in the Internet
- Privacy

8.1 Trust in the Internet

Definition

While the focus of CSIA R&D is necessarily on technical advances that improve cyber security and information assurance, such technical activities take place within a broader cultural context: the overall level of public confidence, or trust, in the Internet and the varied transactions and processes it makes possible. Public trust in the Internet can be defined as the degree to which individuals and organizations feel

stages of development are more easily mitigated with reduced impact on the development effort. Resources and tools can include privacy-impact assessments and privacy audits, which together can establish objectives and evaluate privacy throughout the life cycle of the system and its data.

Privacy principles: The private sector, government, and citizens are each subject to privacy laws, regulations, and/or practices. Cyber security R&D should enable new technologies and their implementation to be consistent with privacy laws and widely accepted privacy principles. Examples include principles for assuring data quality and integrity; limits on data collection, use, disclosure, and retention; openness and accountability; and citizen participation and impact through notifications, accessibility, and avoiding or redressing harm from inaccurate data.

Privacy environments: The technical environments for privacy in cyber security are of two primary types: 1) the maintenance environment, which involves system architecture and the storage and protection of data; and 2) the transaction environment, which concerns how data are shared and exchang-18.116 6cy in jT* 7rit0nd 2anizicatioes. Cyber security and (fmipation assenancy R (shouladredreor privand)TjT* aspleraisng-by bowity typre ol environmen.th)Tj0 -1.7435 Tw(The m privacfeaectusne of tseow technologiewillnbarareeo udof

Appendices

This appendix provides brief descriptions of the missions of the Federal agencies that participate in the Cyber Security and Information Assurance Interagency Working Group (CSIA IWG) as well as summaries of their CSIA R&D activities and interests.

Department of Commerce (DOC) and National Institute of Standards and Technology (NIST)

Building upon the Computend

intelligence, surveillance, and reconnaissance. All of these capabilities must be supported by an underlying foundation of information assurance to facilitate "decision superiority" on the battlefield. Successful application of these capabilities will enable full-spectrum dominance for U.S. forces in the future.

The DoD Science & Technology (S&T) program advances the S&T base for protecting critical defense infrastructures and develops tools and solutions to eliminate any significant vulnerability to cyber attacks. The program includes thrusts in the areas of analysis and assessment, mission assurance, indications and warning, threats and vulnerabilities, remediation, mitigation response, and reconstitution. The program focuses on DoD requirements for protection that go well beyond what the private sector requires and commercial technologies provide.

The Director for Defense Research and Engineering (DDR&E) is responsible for DoD S&T. The DDR&E is also the Chief Technology Officer for the Secretary of Defense and the Under Secretary of Defense for Acquisition, Technology, and Lciastics

agencies. FAA's unique requirements are based on identification of security measures that provide for the safety and security of the FAA workforce, facilities, and critical infrastructure. Cyber-defense concept modeling plays a significant role in improving the security of FAA's information infrastructure. The agency's cyber security goal is mission survivability by achieving zero cyber events that disable or significantly degrade FAA services. The Director of

The Networking and Information Technology Research and Development (NITRD) Program is authorized by Congress under the High-Performance Computing (HPC) Act of 1991 (P.L. 102-194) and the Next Generation Internet Research Act of 1998 (P.L. 105-305). The goals of the Program are to:

- Provide research and development foundations for assuring continued U.S. technological leadership in advanced networking, computing systems,

essential for the operation and evolution of the country’s national defense, key industrial sectors, and critical infrastructures.

The HCSS Coordinating Group coordinates the activities of the HCSS PCA.

Social, Economic, and Workforce Implication 47, 9nbls234 -1, 2 TD ofIT, andIT, WorkforceDevelopmsen (SEW)9

The(activitiesfunded undeor theSEWS PCI fcues ne)Tj0 -1.2 TD theinatur, anddynaomies ofIT, andits iImplicationd

apabilvitie;r thewWorkforcedevelopmsen needes ristind

anl inormrsSociaepopliy maktin,dIT,designrs, theITe

TheSEWS Coordinating Group coordinates the activities of theSEWS PC. .

Sftw re Designn andProducctiviy (SDP)9

and

TheSDP,R&D8agenda spaon bothd
e.g.,d

e.g.,,projeca m aagemsen,d

LABS -

The *Federal Plan for Cyber Security and Information Assurance Research and Development* is the product of extensive efforts by the co-chairs and members of the Interagency Working Group (IWG) on Cyber Security and Information Assurance. In addition, experts not formally affiliated with the IWG provided specialized technical information and feedback on drafts that were also essential to the completion of this Plan.

The National Coordination Office for Networking and Information Technology Research and Development played an instrumental role in the Plan's development, Cover Design, Graphics, and Printing