NITRD CSIA IWG
Cybersecurity Game-Change
Research & Development Recommendations

Introduction

The President's Cyberspace Policy Review challenges the Federal community to develop a framework for research and development strategies that focus on game-changing technologies that can significantly enhance the trustworthiness of cyberspace.

The Cybersecurity Game-Change Research and Development (R&D) Recommendations, coordinated through the Federal Networking and Information Technology Research and Development (NITRD) Program (www.nitrd.gov) and its Cyber Security Information Assurance (CSIA) Interagency Working Group (IWG), have identified three (3) initial R&D themes to exemplify and motivate future Federal cybersecurity research activities: (a) Moving Target, (b) Tailored Trustworthy Spaces, and (c) Cyber Economic Incentives. While these themes do not themselves constitute a prioritized research agenda, they inspire new and different ways of thinking about problems and provoke novel solutions to develop technologies that provide increases in cybersecurity.

These three themes challenge some of the fundamental assumptions that have traditionally provided a foundation for cybersecurity research and, in doing so, offer the promise of changing the game in cybersecurity. The intent is not to aspire to develop the perfectly secure system, or to hope to develop universally useful security mechanisms that satisfy all cybersecurity needs. Rather, the aim is to develop methods that elude attackers, to focus on systems tailored to address risks relevant to specific information and transactions, to create an economic framework that identifies the motivations of cyber users and to develop market forces that incentivize good behavior. This attention shift is motivated by an understanding of the extreme dynamism and complexity of cyberspace and is based on the following hypotheses:

- The cost of attack is asymmetric, and favors the attacker. Defenders must exponentially increase the cost of attack and must employ methods that enable them to continue to operate in the face of attack.

- The cost of simultaneously satisfying all the cybersecurity requirements of an ideal system is prohibitive. Sub-spaces must be enabled to support varying security policies and services for different types of interactions.

- The lack of meaningful metrics and economically sound decision making in security results in a misallocation of resources. Economic principles must be promoted that encourage the broad use of good cybersecurity practices and deter illicit activities.

End-State

Securing the U.S. cyber infrastructure requires a dynamic understanding of the totality of its complexities. The following recommendations aim to justify R&D that supports the overall strategy:

- Improve techniques for managing network presences to make cyber assets a moving target in cyberspace. This will require increased sophistication on the part of would-be attackers.

- Create a trustworthy cyberspace model with observable metrics such that abnormalities, be they the result of attack, physical disaster, accident or routine failures, can be readily identified and remediated. Analytics and self-aware discovery methods are necessary to provide early warning of even the most determined adversaries' activities and convincing attribution to support retaliation. Smart data will protect itself from exploitation. New methods will enable us to assess the health and trustworthiness of our systems and environment and smartly control our cyber interactions. Improved infrastructure resilience will enable us to operate securely during an attack, and will provide resistance to outages caused by physical disasters, accidents, and routine system failures. Trustworthy cyberspace will allow users to operate safely even in the presence of compromise.

- Create a framework of economic incentives to reward secure practices and discourage bad actors. The cost of attack will be proportionate to the value of the information or the system, so only the most determined adversaries will consider attack an option worth pursuing. Improved methods of accountability (including attribution) appropriate to the context of use and deterrence policies will make attacks less attractive for those who rely on anonymity and the absence of consequences for their safety.

These research recommendations are focused on influencing FY 2012 funding decisions and are organized around the Moving Target, Tailored Trustworthy Spaces, and Cyber Economic Incentives themes. Each theme includes a vision statement and explanation of the game-changing idea. Additionally, each theme identifies goals, challenges, research milestones, critical supporting technologies, non-technical barriers, and for one theme, use-cases. The research milestones have been divided into: (a) near-term (low complexity, capability demonstration within 18 months), (b) mid-term (medium complexity, capability demonstration within 36 months), and (c) long-term (high complexity, high risk).

Moving Target

Research into Moving Target (MT) technologies will enable us to create, analyze, evaluate, and deploy mechanisms and strategies that are diverse and that continually shift and change over time to increase complexity and cost for attackers, limit the exposure of vulnerabilities and opportunities for attack, and increase system resiliency. The characteristics of an MT system are dynamically altered in ways that are manageable by the defender yet make the attack space appear unpredictable to the attacker. MT technology changes the game by wresting the advantage from the attacker because it eliminates the availability of constant or slowly-changing vulnerability windows that allow attackers to lie in wait and conduct useful experiments on persistent vulnerabilities.

This game-changing approach challenges the traditional approach which counsels that adding complexity to our systems also adds risk. Conversely, the complexity of today's computational platforms and analytic and control methods can now be used to frustrate our adversaries. The challenge is to demonstrate that complexity is indeed a benefit and not a liability.

Research is required to:

- Develop abstractions and methods that will enable scientific reasoning regarding MT mechanisms and their effectiveness
- Characterize the vulnerability space and understand the effect of system randomization on the ability to exploit those vulnerabilities
- Understand the effect of randomization of individual components on the behavior of complex systems, with respect to both their resiliency and their ability to evade threats.
- Develop a control mechanism that can abstract the complexity of MT systems and enable sound, resilient system management
- Enable the adaptation of MT mechanisms as the understanding of system behavior matures and our threat evolves

The MT area has its underpinnings in fundamental research in the following supporting or component areas: virtualization, multi-core processing, new networking standards, cryptography, system management, software application development, and health-inspired or evolutionary resiliency and defense methods.

Moving Target R&D Plan

Vision:

Create, evaluate, and deploy mechanisms and strategies that are diverse, continually shift, and change over time to increase complexity and costs for attackers, limit the exposure of vulnerabilities and opportunities for attack, and increase system resiliency.

Why is this a Game Change:

Currently, attackers have the advantage to exploit our systems. The systems we use are deterministic, homogeneous, and static, allowing investments in reconnaissance and attack to pay off due to unchanging vulnerability windows. When vulnerabilities endure, attackers have the ability to lie in wait, develop attacks, and compromise systems at their own pace. System and network administrators are currently in a reactive state of patching and upgrading to secure vulnerable systems. MT strategies aim to substantially increase the cost of attacks by deploying and operating networks and systems in a manner that makes them less deterministic, less homogeneous, and less static.

Goals:

- To design resilient systems that operate reliably in a compromised environment
- To shift from reactive security postures to active preemptive postures
- To create and develop MT mechanisms that are internally manageable, creating disruption for the adversaries, but not for legitimate users
- To analyze the effectiveness of MT mechanisms against various attacks and disruptions, in relation to applicable environments
- To increase the ability to observe, shape, and expose the actions of adversaries as they attempt to break MT mechanisms

Challenges:

- Develop abstractions and methods that will enable scientific reasoning about MT mechanisms and their effectiveness
- Identify system characteristics and the degrees of their movement, in terms of both entropy and movement intervals, where MT mechanisms are most effective
- Develop MT management methods that allow systems to work without failure and that can maintain interoperability with legacy systems and technologies
- Perform a cost-benefit analysis that considers the additional cost to adversaries and defenders
- Create MT mechanisms that can evolve and adapt, increasing their effectiveness
- Evolve the ecosystem of programming languages, tools, architectures, evaluation and testing methodologies, and operational controls to support proven MT mechanisms; institutionalize best concepts and practices through computer science education

- Interactions with legacy systems: Legacy systems can encompass many different types of technologies, systems, computers, and equipment. When implementing a MT mechanism, the existing methods must simultaneously continue to fully operate on that system.

Milestones

Strategy	Near-term milestones	Mid-term milestones	Long-term milestones
Create	Create one or more new MT mechanisms within one system dimension.	Provide integrated operation of two or more separate MT mechanisms that work in different system dimensions.	Create one or more MT mechanisms that span multiple system dimensions.
	Create a framework for MT mechanism management on a limited network.	Develop movement synchronization and more complex system management.	Create one or more MT mechanisms that can evolve and adapt over time independently.
Evaluate / Analyze	Establish techniques to evaluate the effectiveness of proof-of-concept MT mechanisms.	Enable component-level and whole system evaluation of MT solutions across diverse operating environments.	Enable real-time analysis of MT effectiveness in support of movement adaptation.
	Simulate, test, and evaluate existing approaches, algorithms, and prototypes for MT.	Develop capability to model, simulate, test, and evaluate MT solutions at enterprise scale.	Develop capability to model, simulate, test, and evaluate all types of MT solutions at Internet scale.
Deploy	Deploy at least one MT mechanism in a controlled environment of a national R&E network with instrumentation and performance evaluation.	Deploy multiple MT techniques in controlled enterprise-level environments.	Achieve broad and diverse commercial availability and adoption of multiple MT solutions and systems.

Critical Supporting Technologies:

- Virtualization: Virtualization has become widely used in enterprise environments, delivering a range of operational, management, and cost benefits. Virtualized environments can provide a building block for enabling and deploying MT solutions.
- Multi-core processing: The shift from more powerful individual cores to multiple processing cores provides opportunities for improving the effectiveness of MT mechanisms.
- New networking standards: Elements of networking constitute one or more system dimensions upon which MT mechanisms can be implemented. New standards and protocols may be required to allow MT solutions.
- Cryptography: Some MT mechanisms utilize cryptographic keys and key management to synchronize movement. Enhanced key management and low latency cryptographic methods will be required for complex MT systems.

Critical Supporting Technologies (continued):

- System Management: MT mechanisms have the potential side effect of disrupting the operation of our systems. The ability to manage a system that incorporates MT mechanisms will therefore be a greater challenge.

- Software Application Development: Programming languages and methods need to be developed to support MT techniques and increase their effectiveness.

- Health-Inspired MT Methods: Health-inspired and evolutionary methods can enable systems that evolve over time, like that of biological organisms. MT mechanisms should incorporate and enhance advances in this area to create more effective methods.

- Assessment of Existing Research: Prior promising research in MT strategies and mechanisms may not have been feasible due to limited computational resources. Advancements in computing may now permit implementation of such ideas; feasibility analysis should be done to identify and assess prior research.

Potential Non-Technical Barriers:

- Public Education of Mechanisms: Education is required to build understanding of, and public trust in, MT mechanisms facilitated by open methods that do not rely on obscurity for their security.

- Liability Policy: With the implementation of an MT mechanism, who becomes liable if the technology fails or disrupts our current operations? Does the supplier of the mechanism become fully liable? Does the user become liable when the user implements the mechanism in different fashions? Liability becomes a serious problem for MT that must be well thought out.

Tailored Trustworthy Spaces

Tailored Trustworthy Spaces (TTS) provide flexible, adaptive, distributed trust environments that can support functional and policy requirements arising from a wide spectrum of activities in the face of an evolving range of threats. A TTS recognizes the user's context and evolves as the context evolves. The user chooses to accept the protections and risks of a tailored space, and the attributes of the space must be expressible in an understandable way to support informed choice and must be readily customized, negotiated and adapted.

The power of the tailored spaces theme lies in the capability to:

- Articulate and negotiate the security requirements of the situation at hand
- Adjust the assurance level on specific security attributes separately
- Establish trust between systems based on verifiable information that test the limits of traditional trust policy articulation and negotiation methods, raising the bar for highly dynamic human understandable and machine readable assured policies. This necessitates the development of dependable methods of separating and isolating processes operating from small trust islands in a largely untrustworthy system

The primary goal of the tailored spaces theme is to identify and develop a common framework that supports varying trustworthy space policies and services for different types of actions. These policies and services will provide visibility into rules and attributes of the space to inform trust decisions, a context specific set of trust services, and a means for negotiating the boundaries and rules of the space. This framework will offer assurance that user requirements are accurately articulated in the TTS policy, that these spaces are truly separate, and that build-up and tear-down of the space is clean and trustworthy.

The scientific challenge of tailored spaces is to provide the separation, isolation, policy articulation, negotiation, and requisite assurances necessary to support specific cyber sub-spaces. Research is required to develop:

- Trust negotiation tools and data trust models to support negotiation of policy
- Type-safe languages and application verification, tools for establishment of identity or authentication as specified by the policy
- Data protection tools, access control management, monitoring and compliance verification mechanisms to allow for informed trust of the entire transaction path
- Resource and cost analysis tools
- Hardware mechanisms that support secure bootload and continuous monitoring of critical software
- Least privilege separation kernels to ensure separation and platform trust in untrustworthy environments
- Application and operating systems elements that can provide strong assurance that the program semantics cannot be altered during execution
- Support for application aware anonymity to allow for anonymous web access; and platform security mechanisms and trust-in-platform establishment

Tailored Trustworthy Spaces R&D Plan

Vision:

Create flexible, distributed trust environments that can support the functional and policy requirements arising from a wide spectrum of activities in the face of an evolving range of threats. Tailored Trustworthy Spaces (TTS) support a variety of operating capabilities across multiple dimensions, including: confidentiality, anonymity, data and system integrity, provenance, availability, and performance.

Why is this a Game Change:

TTS enable cyber users to make informed trust decisions based on verifiable security properties of their environments and transactions. Today, cyberspace is composed of subsystems that lack mechanisms to ascertain their security conditions and to participate in creating environments with required trust and provenance characteristics. The absence of mechanisms to establish trust has made cyberspace vulnerable to illicit exploitations. A TTS is a vision of transparent secure trust environments suited to users' context. In the future, users and systems will have the means to establish a TTS by invoking and tailoring a set of security attributes to create a work environment within cyberspace appropriate to the task at hand. The establishment of trust between participants and systems in TTS will be based on verifiable information and properties.

Goals:

- Develop mechanisms to enable specific trustworthy space policies and services for specific types of actions:
    a) Allow rules, attributes, and boundaries of the space to be defined to inform trust decisions.
    b) Ensure that requirements for the use case can be accurately articulated in the policy for the TTS.
    c) Establish a context specific set of trust services, supported by a scalable set of tools.
    d) Assure a proper separation of spaces so that the build-up and tear-down of the spaces is trustworthy.

- Enable trustworthy computing in untrustworthy environments.

Challenges:

- Develop rules, measurable metrics of trustworthiness, flexible trust negotiation tools, configuration decision support capabilities, and the ability to perform informed trust analysis.

- Develop a scalable service framework.

- Ensure that users' requirements can be enabled in the policies that control the TTS, and that the policies can be implemented by relevant elements of the TTS.

- Assure separation, and prevent leakage, of information between spaces.

- Ensure that threat identification and mitigation will be considered in the policy and methods of defining TTS.

Milestones			
Attribute	**Near-term milestones**	**Mid-term Milestones**	**Long-term Milestones**
1-TTS characterization	Specify TTS elements. Identify existing standards.	Submit RFCs for new or revised standards to support TTS.	Establish interoperable standards for defining TTS for multiple use cases.
2-Translation of requirements into TTS policies	Develop models and tools to specify tailoring requirements. Define system-, service- or human- to TTS interface.	Translate tailoring requirements into rules and policies. Enable user/service visibility into the rules/policies.	Provide assurance that all and only the requirements that match the use case, are accurately articulated in the policy for the TTS.
3-Trust negotiation and TTS Establishment	Deploy predefined trust capabilities (canned preset spaces). Deploy a pilot of an anonymous TTS, a low assurance, and a high assurance TTS.	Demonstrate tailorable trust negotiation of multiple attributes.	Achieve dynamically tailorable trust transactions.
4-Threat assessment and analysis to improve tailoring	Identify relevant threat vectors. Conduct impact assessment. Develop impact mitigation approaches.	Develop methods to tailor a TTS given a threat scenario.	Provide capabilities for informed tailored threat mitigation including conventional and enhanced protection services (i.e. MT).
5-TTS operations (joining, adjusting, dynamically tailoring a TTS)	Provide capability to join an existing TTS. Define process needs for operating an existing space. Define process needs for maintaining an existing space.	Identify and define process needs for adjusting an existing TTS. Develop capability to adjust an existing TTS.	Provide capabilities to set up and tear down dynamic TTS, to split or merge TTS spaces, and to define and manage interaction between TTS spaces.
6-Assured separation of spaces	Define space isolation policies. Define space to space movement.	Provide assurance that data stays within defined space boundaries.	Achieve verifiable separation of spaces.
7-Value Analysis	Establish models and methods for analysis of benefits of TTS.	Develop models and methods that incorporate value analysis into trust negotiations.	Enable dynamic cost-benefit analysis of TTS.

Critical Supporting Technologies:

- Trust negotiation tools: trust negotiation protocol elements, tailored identity establishment and management, transaction attribution mechanisms, reference monitors.
- Access control management, monitoring and compliance verification mechanisms to allow for informed trust of the entire communication path (limited by the TTS policy).
- Data trust models to support negotiation of TTS policy based on data criticality.
- Validation tools to provide the ability to verify application configuration and functions conform to the policy and as expected.
- Data encryption and protection tools to support stronger non-repudiation and data attribution
- TTS resource and cost analysis tools.
- Hardware mechanisms to establish trusted state and to monitor critical software.
- Least privilege separation kernels to ensure separation and platform trust in untrustworthy environments.
- Application and operating systems elements (programming languages and compilers) that can provide assurance that the program semantics cannot be altered during execution.
- Network and hardware configuration verification of TTS rules to establish trusted paths.

Potential Non-Technical Barriers:

- Education/Introduction to Tailored Space: The public understands the importance of privacy and security; however many will not comprehend that the application of trust technologies can be tailored to the skill level of the user and the activity being accomplished by that user. Information on the benefits of this tailoring and mechanisms that provide assurance that tailoring has been implemented correctly, may be required.
- Implementation of the user-to-TTS interface: The ability to accurately capture and incorporate user needs into TTS policy, is an important precondition to a successful TTS implementation.
- Liability Policy: If TTS adapts policy and security features based on the task at hand, is there liability if the mechanisms selected are not appropriate to the task? This is a valid concern in any automated process and the "informed trust" that TTS will provide needs to be implemented such that the user maintains control and responsibility for the level of protection/trust of the space.

Use Case Examples:

- Anonymous Health Care or Employment search web surfing for private purposes where attribution and authentication are not desirable.
- Protection of personal medical history or lab reports between individuals with minimal IT infrastructure and medical or insurance providers with substantial IT infrastructure.

Use Case Examples (continued):

- Creation of an environment within cyberspace that can be trusted with sharing of information between government agencies as well as with coalition partners and state, local, and tribal authorities.
- Authenticated, audited government-to-government transactions such as E-Gov or GAO reporting, and interagency sharing of sensitive information.
- Capability to leverage TTS for the exchange of controlled and authenticated, high value messages such as those which support large financial transactions, official government dispatches, and military orders.
- Demonstration of the ability to handle confidential authenticated citizen-to-government transactions such as submission of tax data, or electronic voting.
- Demonstration that a high assurance tailored space suitable for national security requirements can be established in a trustworthy way.

Cyber Economic Incentives

Cybersecurity practices lag behind technology. Solutions exist for many of the threats introduced by casual adversaries, but these solutions are not widely used because incentives are not aligned with objectives, and resources are not correctly allocated.

Secure practices must be incentivized if cybersecurity is to become ubiquitous, and sound economic incentives need to be based on sound metrics, processes that enable assured development, sensible and enforceable notions of liability and mature cost/risk analysis methods. Without a scientific framework, it is difficult to incentivize good cybersecurity practices and subsequently to make a convincing business case for enhanced cybersecurity mechanisms or processes. The projected benefits must be quantified to demonstrate that they outweigh the costs incurred by the implementation of improved cybersecurity measures. There are no sound metrics to indicate how secure a system is, so one cannot articulate how much more secure it would be with additional investment. There is no scientific basis for cost/risk analysis, and business decisions are often based on anecdotes or un-quantified arguments of goodness. Currently, it is also very difficult to collect the large body of data needed to develop a good statistical understanding of cyberspace without compromising the privacy of individuals or the reputation of companies. The means to identify and re-align cyber economic incentives and to provide a science-based understanding of markets, decision making, and motivators must be investigated.

Research is required to:

- Explore models of cybersecurity investment and markets
- Develop data models, ontologies, and automatic means of anonymizing or sanitizing data
- Define meaningful cybersecurity metrics and actuarial tables
- Improve the economic viability of assured software development methods; provide methods to support personal data ownership
- Provide knowledge in support of laws, regulations and international agreements

Cyber Economic Incentives R&D Plan

Vision:

Promote the role of economics in identifying and realigning cyber economic incentives by creating a science-based understanding of markets, decision making, and motivators; promote an environment where deployment of security technology is balanced, providing incentives to engage in socially responsible behavior and deter those who participate in criminal and malicious behavior.

Why is this a Game-Change:

A focus on the economics of cybersecurity is a recognition that information security problems are substantially issues of misaligned incentives and misallocated resources - and are therefore economic problems that require economic and not merely technical solutions. Today cyber-crime pays. Criminal activities are attractive because the cost to engage in them is small compared with their projected return on investment. Understanding the structures of costs and incentives is crucial in order to motivate cyber participants to take actions in ways that improve overall security.

Goals:

- Enable economic analyses and operational action by establishing trusted repositories of cyberspace data (e.g., usage, incidents, attacks, losses) and metrics.
- Develop new theories and models of cyber economics and scientific understanding of the social dimensions of cyber economics.
- Develop a scientific framework to incentivize vendors of cyberspace-related technologies (e.g., encourage use of secure software engineering and analysis practices, software vulnerability detection, security incident forensics) through acquisition, regulation, and standards.
- Promote an environment where (1) users are well informed about cyber security, so that they reward vendors that provide secure products and services, and (2) individuals have “ownership” of their personal data, are aware of its provenance, and control its authenticated and authorized distribution, use, destruction with greater understanding of the economic value of such data.
- Empower cyberspace service providers (e.g., Internet Service Providers, Application Service Providers, registrars, registries, banks, countries, nation-states, etc.) to reduce abusive or criminal behavior and to provide the means to better defend services and systems against abuses and exploitation, while offering the appropriate legal/regulatory framework (e.g., exemptions, liability protection) and law enforcement support.

Challenges:

- Lack of legal and ethical collection, protection, and distribution of cyberspace data.
- Lack of appropriate data to support effective economic analysis (e.g., insurance actuarial information, incident trending evaluation).
- Lack of understanding and agreement about “personal data”, its ownership, accountability, and its usage in an environment that is currently self-regulating and driven by market-based solutions.

Challenges (continued):

- Establish a neutral operational entity with appropriate authorities to conduct investigations and produce authoritative findings.
- Educate users about the benefits of secure practices and cyber behavior.
- Understand the economic benefit of protecting critical infrastructure against disruption and educate vendors about their role in protecting critical infrastructure and the consequences of failures in this domain.
- Determine the scope of action allowed by service providers and the boundaries between service provider empowerment and law enforcement involvement, within the context of their global legal capacities and partnerships.

Milestones

Attribute / Approach	Near-term milestones	Mid-term milestones	Long-term milestones
Theories and Models	Analyze current models of cybersecurity investment and usage to determine future economic drivers. Develop economic models to encourage potential data providers to provide data.	Develop economic-based science and theories that will change current behaviors with respect to usage of cybersecurity technologies.	Incentivize usage of solutions that are based on new economic-based science and theory.
Data and Metrics	Establish priority goals for economic analyses and identify data to be collected and define metrics (ongoing). Determine the utility of the data collected (ongoing). Determine a methodology to collect/distribute data (policy legal/technical implications). Identify metrics for assessing the “vulnerability resiliency” of software. Identify past examples of relationships between incidents and economic impact.	Develop ontologies (metadata, annotation, etc.) for data. Refine incident-to-economic-impact models and test them against past data. Develop methodologies to automatically compute relationships between incident data, economic impact, and value of defense.	Achieve automatic anonymization and sanitization of data without destroying utility of data. Enable automatic determination of relationships between incident data and economic impact to synthesize defenses. Establish economic models of security and actuarial science of trustworthiness.

Vendor Incentives	Define what it is that vendors should be required to satisfy, e.g., which methodologies and internal processes should be incorporated into their product development cycles. Determine opportunities to change government regulatory and acquisition laws (e.g. CFR, FAR) and guidance for both safety and cyber security impacts. Assess the capabilities of existing tools against agreed-upon evolving benchmarks. Define models where vendors will benefit from using tools (requires economic model and regulatory intervention, including third-party software vendors).	Improve existing software quality tools (usability, efficiency, and capability). Institutionalize education of vendors and the public about the economic benefits of using "safe" software. Develop and enforce "safety meters" on popular applications making users aware of the risks of the software they use.	Develop new tools for improving software quality. Develop automatic "meters" for safety and vulnerability resistance of software on all applications.
Personal Data Ownership	Develop definitions and metrics of privacy and "personal data ownership." Develop models for data provenance lifetimes.	Develop private data provenance standards / requirements (data privacy reputation). Define boundaries between personal, corporate, and open data ownership models.	Deploy infrastructure (such as proper provenance) that enables control/awareness by its owner(s) of the use of their personal data.
Infrastructure Empowerment	Study the legal and technical issues and barriers involved in data sharing among service providers, both domestic and global. Demonstrate learning of "attack signatures" from consolidated data provided by service providers. Analyze current data sharing among international partners.	Develop models to assess economic impact of new laws and regulations associated with data sharing. Develop improved models for domestic and international collaboration and data sharing.	Implement new models of international collaboration and data sharing.
Critical Supporting Technologies: • Decide what data to collect, how to store it, and how to share it. • Determine appropriate metrics.			

Critical Supporting Technologies (continued): • Develop relevant economic models for cost/benefit and insurance analysis. • Create specification (and evaluation) baselines for software and technology verification and validation processes and mechanisms.
Potential Non-Technical Barriers: • Determination of the right public/private boundary for security enforcement.

Enablers of Technology Diffusion and Adoption

Given the pressing need to address the problems of cyber security, it is expected that many game-changing results will move rapidly from concept to practice. For projects that clearly demonstrate that such a transition to practice is likely, contracts can require technology transfer. For other projects, researchers can be encouraged to inform their teams about opportunities to incubate their nascent ideas in a setting that is conducive to achieving this goal.

Some researchers are accomplished innovators and also accomplished at finding solutions to hard game-changing problems, but have little interest in commercializing the resulting solutions. In such cases, several steps can be taken. First, incubators can be funded that are designed to attract and assist team members who find this type of work interesting and rewarding. Second, other researchers who are not associated with development of the solutions can be funded to transition ideas to the next phase of development. As part of the incubation process, funding agencies should point contractors to sources of Federal start-up funds.

Industry-based research consortia have proven effective in focusing attention on research priorities, bringing researchers together, and funding their activities. Consortia targeting game-changing research topics can play a very effective role in advancing the research agenda. In addition to providing directed funding, they can also sponsor contests and serve as vehicles to provide recognition for major contributors. Federal agencies can provide seed funding for such consortia.

Universities have responsibility under the Bayh-Dole Act of 1980 to protect the intellectual property produced with Federal funding as well as to commercialize it, if possible. While research universities acknowledge these obligations and a few are very successful, most find it a challenge. Funding agencies can help by encouraging universities to create industrial partner programs designed to stimulate pre-competitive cooperation among industrial partners. Such programs also help students to appreciate the problems of industry as well as expose them to potential employment opportunities. Funding for curricular development in game-changing areas can also stimulate student interest.

Since the problems of cyber security are challenging, funding for basic long-term research is essential. The measures described above should be overlaid on such research but not to the extent that the basic objectives for secure computation are lost.

Federal agencies can increase their effectiveness by creating, in consultation with professional societies, incentive systems designed to bring individuals of high achievement and good judgment into government service as program managers. Given the vital role these individuals play, it is important that the best and brightest be recruited. The agencies can also work with these organizations to develop technology transitions programs best suited to the technologies in question. Finally, agencies can use their purchasing power to encourage the adoption of game-changing technology standards, when ready.

Connection to the Comprehensive National Cybersecurity Initiative (CNCI) and the National Cyber Leap Year

Initiative number nine of the Comprehensive National Cybersecurity Initiative (CNCI) tasks the USG Cybersecurity R&D community to define and develop enduring "leap-ahead" technology, strategies, and programs. One goal of the CNCI is to develop technologies that provide increases in cybersecurity by orders of magnitude above current systems and which can be deployed within five to ten years. The initiative seeks to develop strategies and programs to enhance the component of the government R&D portfolio that pursues high-risk/high-payoff solutions to critical cybersecurity problems. These recommendations represent NITRD CSIA IWG's identification of common needs that should drive mutual investment in key research areas.

The three themes recommended should be viewed as encompassing aspects of the initial five topics that were discussed during the National Cyber Leap Year Summit held in August 2009 (http://www.nitrd.gov/NCLYSummit.aspx):

- Digital Provenance - basing trust decisions on verified assertions
- Moving-target Defense - attacks only work once if at all
- Hardware-enabled Trust - knowing when we've been had
- Health-inspired Network Defense - move from forensics to real-time diagnosis
- Cyber Economics - crime doesn't pay

Summary

Achieving enduring trustworthiness within cyberspace requires new paradigms that re-balance the security asymmetries of today's landscape: the cost of simultaneously satisfying all the requirements of an ideal cybersecurity solution is impossibly high, and so we must enable sub-spaces in cyberspace to support specific security policies and services for specific types of interactions; the cost of attack is asymmetric, favoring the attacker, and so defenders must increase the cost of attack and must employ methods that enable them to continue to operate in the face of attack; the lack of metrics and economically sound decision making in security misallocates resources. Thus economic principles must be promoted that encourage the broad use of good cybersecurity practices and deter illicit activities.

The NITRD CSIA IWG believes that a research agenda should be constructed that initially focuses on the three themes and enables technologies required by these themes. As the public sector pursues this research, and, more importantly, as the public sector engages the private sector with these themes, we expect new themes will emerge, enriching the understanding of how to build a more trustworthy cyberspace.

The NITRD CSIA IWG recognizes that the three themes are not all-encompassing, nor do they provide a complete Leap Ahead vision for U.S. Cyberspace. The NITRD CSIA IWG will be establishing Internet based mechanisms to allow industry and academic communities to provide input that can impact cybersecurity R&D funding for FY12 and beyond.