Office Of The Secretary Of Defense (OSD)
Deputy Director Of Defense Research & Engineering
Deputy Under Secretary Of Defense (Science & Technology)
Small Business Innovation Research (SBIR)
FY2007.2 Program Description

Introduction

The Deputy Under Secretary of Defense (Science & Technology) SBIR Program is sponsoring the Information Assurance theme and the Cognitive Readiness theme this solicitation.

The Army, Navy, Air Force, and SOLIC are participating in the OSD program this year. The service laboratories act as our OSD Agent in the management and execution of the contracts with small businesses. The service laboratories, often referred to as a DoD Component acting on behalf of the OSD, invite small business firms to submit proposals under this Small Business Innovation Research (SBIR) program solicitation. In order to participate in the OSD SBIR Program this year, all potential proposers should register on the DoD SBIR website as soon as you can, and should follow the instruction for electronic submittal of proposals. It is required that all bidders submit their proposal cover sheet, company commercialization report and their firm's technical and cost proposal form electronically through the DoD SBIR/STTR Proposal Submission Website at http://www.dodsbir.net/submission. If you experience problems submitting your proposal, call the help desk (toll free) at 1-866-724-7457. You must include a Company Commercialization Report as part of each proposal you submit; however, it does not count against the proposal page limit. Please note that improper handling of this form may result in the proposal being substantially delayed. Information provided may have a direct impact on the review of the proposal. The DoD SBIR Proposal Submission Website allows your company to come in any time (prior to the proposal submission deadline) to edit your Cover Sheets, Technical and Cost Proposal and Company Commercialization Report.

We <u>WILL NOT</u> accept any proposals that are not submitted through the on-line submission site. The submission site does not limit the overall file size for each electronic proposal, there is only a page limit. However, file uploads may take a great deal of time depending on your file size and your internet server connection speed. If you wish to upload a very large file, it is highly recommended that you submit prior to the deadline submittal date, as the last day is heavily trafficked. You are responsible for performing a virus check on each technical proposal file to be uploaded electronically. The detection of a virus on any submission may be cause for the rejection of the proposal. We will not accept e-mail submissions.

Firms with strong research and development capabilities in science or engineering in any of the topic areas described in this section and with the ability to commercialize the results are encouraged to participate. Subject to availability of funds, the DUSD(S&T) SBIR Program will support high quality research and development proposals of innovative concepts to solve the listed defense-related scientific or engineering problems, especially those concepts that also have high potential for commercialization in the private sector. Objectives of the DUSD(S&T) SBIR Program include stimulating technological innovation, strengthening the role of small business in meeting DoD research and development needs, fostering and encouraging participation by minority and disadvantaged persons in technological innovation, and increasing the commercial application of DoD-supported research and development results. The guidelines presented in the solicitation incorporate and exploit the flexibility of the SBA Policy Directive to encourage proposals based on scientific and technical approaches most likely to yield results important to DoD and the private sector.

Description of the OSD SBIR Three Phase Program

Phase I is to determine, insofar as possible, the scientific or technical merit and feasibility of ideas submitted under the SBIR Program and will typically be one half-person year effort over a period not to exceed six months, with a dollar value up to $100,000. We plan to fund 3 Phase I contracts, on average, and downselect to one Phase II contract per topic. This is assuming that the proposals are sufficient in quality to fund this many. Proposals should concentrate on that research and development which will significantly contribute to proving the scientific and technical feasibility of the proposed effort, the successful completion of which is a prerequisite for further DoD

support in Phase II. The measure of Phase I success includes technical performance toward the topic objectives and evaluations of the extent to which Phase II results would have the potential to yield a product or process of continuing importance to DoD and the private sector, in accordance with Section 4.3.

Subsequent Phase II awards will be made to firms on the basis of results from the Phase I effort and the scientific and technical merit of the Phase II proposal in addressing the goals and objectives described in the topic. Phase II awards will typically cover 2 to 5 person-years of effort over a period generally not to exceed 24 months (subject to negotiation). Phase II is the principal research and development effort and is expected to produce a well defined deliverable prototype or process. A more comprehensive proposal will be required for Phase II.

Under Phase III, the DoD may award non-SBIR funded follow-on contracts for products or processes, which meet the component mission needs. This solicitation is designed, in part, to encourage the conversion of federally sponsored research and development innovation into private sector applications. The small business is expected to use non-federal capital to pursue private sector applications of the research and development.

This solicitation is for Phase I proposals only. Any proposal submitted under prior SBIR solicitations will not be considered under this solicitation; however, offerors who were not awarded a contract in response to a particular topic under prior SBIR solicitations are free to update or modify and submit the same or modified proposal if it is responsive to any of the topics listed in this section.

For Phase II, no separate solicitation will be issued and no unsolicited proposals will be accepted. Only those firms that were awarded Phase I contracts, and have successfully completed their Phase I efforts, will be invited to submit a Phase II proposal. Invitations to submit Phase II proposals will be released at or before the end of the Phase I period of performance. The decision to invite a Phase II proposal will be made based upon the success of the Phase I contract to meet the technical goals of the topic, as well as the overall merit based upon the criteria in section 4.3. DoD is not obligated to make any awards under Phase I, II, or III. DoD is not responsible for any money expended by the proposer before award of any contract. For specifics regarding the evaluation and award of Phase I or II contracts, please read the front section of this solicitation very carefully. Every Phase II proposal will be reviewed for overall merit based upon the criteria in section 4.3 of this solicitation, repeated below:

a. The soundness, technical merit, and innovation of the proposed approach and its incremental progress toward topic or subtopic solution.
b. The qualifications of the proposed principal/key investigators, supporting staff, and consultants. Qualifications include not only the ability to perform the research and development but also the ability to commercialize the results.
c. The potential for commercial (defense and private sector) application and the benefits expected to accrue from this commercialization.

In addition, the OSD SBIR Program has a Phase II Plus Program, which provides matching SBIR funds to expand an existing Phase II contract that attracts investment funds from a DoD acquisition program, a non-SBIR/non-STTR government program or Private sector investments. Phase II Plus allows for an existing Phase II OSD SBIR contract to be extended for up to one year per Phase II Plus application, to perform additional research and development. Phase II Plus matching funds will be provided on a one-for-one basis up to a maximum $500,000 of SBIR funds. All Phase II Plus awards are subject to acceptance, review, and selection of candidate projects, are subject to availability of funding, and successful negotiation and award of a Phase II Plus contract modification. The funds provided by the DoD acquisition program or a non-SBIR/non-STTR government program must be obligated on the OSD Phase II contract as a modification prior to or concurrent with the OSD SBIR funds. Private sector funds must be deemed an “outside investor” which may include such entities as another company, or an investor. It does not include the owners or family members, or affiliates of the small business (13 CFR 121.103).

The Fast Track provisions in section 4.0 of this solicitation apply as follows. Under the Fast Track policy, SBIR projects that attract matching cash from an outside investor for their Phase II effort have an opportunity to receive interim funding between Phases I and II, to be evaluated for Phase II under an expedited process, and to be selected for Phase II award provided they meet or exceed the technical thresholds and have met their Phase I technical goals, as discussed Section 4.5. Under the Fast Track Program, a company submits a Fast Track application, including statement of work and cost estimate, within 120 to 180 days of the award of a Phase I contract

(see the Fast Track Application Form on www.dodsbir.net/submission). Also submitted at this time is a commitment of third party funding for Phase II. Subsequently, the company must submit its Phase I Final Report and its Phase II proposal no later than 210 days after the effective date of Phase I, and must certify, within 45 days of being selected for Phase II award, that all matching funds have been transferred to the company. For projects that qualify for the Fast Track (as discussed in Section 4.5), DoD will evaluate the Phase II proposals in an expedited manner in accordance with the above criteria, and may select these proposals for Phase II award provided: (1) they meet or exceed selection criteria (a) and (b) above and (2) the project has substantially met its Phase I technical goals (and assuming budgetary and other programmatic factors are met, as discussed in Section 4.1). Fast Track proposals, having attracted matching cash from an outside investor, presumptively meet criterion (c). However, selection and award of a Fast Track proposal is not mandated and DoD retains the discretion not to select or fund any Fast Track proposal.

Follow-On Funding

In addition to supporting scientific and engineering research and development, another important goal of the program is conversion of DoD-supported research and development into commercial (both Defense and Private Sector) products. Proposers are encouraged to obtain a contingent commitment for follow-on funding prior to Phase II where it is felt that the research and development has commercialization potential in either a Defense system or the private sector. Proposers who feel that their research and development have the potential to meet Defense system objectives or private sector market needs are encouraged to obtain either non-SBIR DoD follow-on funding or non-federal follow-on funding, for Phase III to pursue commercialization development. The commitment should be obtained during the course of Phase I performance, or early in the Phase II performance. This commitment may be contingent upon the DoD supported development meeting some specific technical objectives in Phase II which if met, would justify funding to pursue further development for commercial (either Defense related or private sector) purposes in Phase III. The recipient will be permitted to obtain commercial rights to any invention made in either Phase I or Phase II, subject to the patent policies stated elsewhere in this solicitation.

Contact with DoD

General informational questions pertaining to proposal instructions contained in this solicitation should be directed to the topic authors and point of contact identified in the topic description section. Proposals should be electronically submitted. Oral communications with DoD personnel regarding the technical content of this solicitation during the pre-solicitation phase are allowed, however, proposal evaluation is conducted only on the written submittal. Oral communications during the pre-solicitation period should be considered informal, and will not be factored into the selection for award of contracts. Oral communications subsequent to the pre-solicitation period, during the Phase I proposal preparation periods are prohibited for reasons of competitive fairness. Refer to the front section of the solicitation for the exact dates.

Proposal Submission

Proposals shall be submitted in response to a specific topic identified in the following topic description sections. The topics listed are the only topics for which proposals will be accepted. Scientific and technical information assistance may be requested by using the SBIR/STTR Interactive Technical Information System (SITIS).

It is required that all bidders submit their proposal cover sheet, company commercialization report and their firm's technical and cost proposal form electronically through the DoD SBIR/STTR Proposal Submission Website at http://www.dodsbir.net/submission. If you experience problems submitting your proposal, call the help desk (toll free) at 866-724-7457. You must include a Company Commercialization Report as part of each proposal you submit; however, it does not count against the proposal page limit. Please note that improper handling of this form may result in the proposal being substantially delayed. Information provided may have a direct impact on the review of the proposal. The proposal submission website allows your company to come in any time (prior to the proposal submission deadline) to edit your Cover Sheets, Technical and Cost Proposal and Company Commercialization Report. We **WILL NOT accept any proposals which are not submitted through the on-line submission site.** The submission site does not limit the overall file size for each electronic proposal, only the number of pages is limited. However, file uploads may take a great deal of time depending on your file size and

your internet server connection speed. You are responsible for performing a virus check on each technical proposal file to be uploaded electronically. The detection of a virus on any submission may be cause for the rejection of the proposal. We will not accept e-mail submissions.

The following pages contain a summary of the technology focus areas, which are followed by the topics.

Cognitive Readiness Technology Focus Area: Understanding the Social, Cultural, and Political Landscape

The successful accomplishment of U.S. national objectives, not just combat objectives, requires US military planners to plan, prepare and conduct operations across many levels of conflict/warfare. When the military deals directly with another nation, area of regard or international coalition, the overall interaction must be framed in the context of the political, military, economic, social, information, and infrastructure. This context directly influences the U.S. government's options (diplomatic, infrastructure, military or economic (DIME), the military's role, and the interagency/intergovernmental relationships within the chosen option(s). Military operational units and the tools that support military planning and execution must be capable of understanding and modeling the effects of humans and human institutions. Social, cultural and geo-political knowledge and models can help define appropriate subordinate objectives and activities for accomplishing National Security goals. The objectives span military strategic and operations planning, military force design, and the development of effective doctrine, tactics, techniques and procedures for accomplishing those objectives. These models and tools also can enable commanders to explore and develop effective integration of shaping activities with those of the kinetic battlefield.

These topics will develop technologies that can be used to develop relevant models that provide new military-relevant capabilities in understanding the social, cultural, and political landscape and how that landscape shapes the ultimate outcome of our combat and non-combat operations. The challenge is to develop both the understanding and framework necessary to improve our ability to plan and prosecute operations in complex geo-political environments.

The Cognitive Readiness Technology topics are:

OSD07-CR1	Getting the Word Out: Modeling the Propagation of Counter Insurgency Information within a Population (SOLIC)
OSD07-CR2	Virtual Iconic Presence (VIP) for Training and Mission Rehearsal (SOLIC)
OSD07-CR3	Training Leaders and Analysts on Measuring Progress in Conflict Environments (MPICE) Tool (Army)
OSD07-CR4	Measuring Progress in Conflict Environments (MPICE) Modeling and Simulation Toolchest and Analysts Work Environment (Army)
OSD07-CR5	Stability Operations Systems Learning Environment (Army)

Information Assurance Technology Area

As envisioned, the GIG will connect the roughly 3 million computers, 100,000 LANs, 100 long-distance networks, and a multitude of wireless networks and devices in support of all DoD, national security, and related intelligence community missions and functions. It will provide the joint warfighter with a single, end-to-end information system capability, built on a secure, robust network-centric environment, allowing users to post and access shared data and applications regardless of their location – while inhibiting or denying an adversary's ability to do the same. The future vision is a converged heterogeneous enterprise capable of protecting content of different sensitivities. However, the GIG construct, while highly desirable from a functionality viewpoint, presents serious challenges from a security perspective. DoD's unprecedented enterprise vision for future information operations must simultaneously address protecting and defending its critical information and information technology systems by ensuring availability, integrity, authentication, confidentiality and non-repudiation; and by providing security management and operations that incorporate the requisite protection, detection, and quick reaction capabilities.

The converged, decentralized vision of the future network requires a parallel adoption of a decentralized trust paradigm. Degrees of trust and robustness hitherto provided by enclave isolation and separation must be distributed across the networks down to the tactical edge devices. With increasing joint, allied and coalition operations, dynamic and secure collaboration and data sharing across security domains are critical capabilities.

DoD is making significant IA investments in ensuring the security of net-centric operations of the GIG. However, the scope of the challenges and the dynamics of the information technology industry provide multiple opportunities for new and innovative security solutions. In particular new technology solutions are needed for supporting the edge users who must operate across multiple domains and communications paths, on less hardened networks, to reach other tactical mission players, and to access protected core information systems and data warehouses.

Topics address the broad technical challenges of developing the technology to ensure fundamental trust of mission critical systems and information (aka Trusting the Edge), to provide the basis for security management (aka Security Management Infrastructure), to enable our customers to transit and/or tolerate a hostile environment to conduct business, including communicate securely, outside the traditional secure enclave (aka Mobility), to enable safe, trusted information exchange (aka Assured Information Sharing), and to provide a seamless, integrated situational awareness capability and rapid, automated protection response capability for the DoD, IC, and National Infrastructure Enterprise Health (aka Enterprise Health: Situational Awareness and Response).

Global Information Grid Information Assurance Research Areas Include:

1. Trusting the Edge
2. Security Management Infrastructure
3. Mobility
4. Assured Information Sharing
5. Enterprise Health

The Information Assurance Technology topics are:

OSD07-I01	Information Dissemination Agent (AF)
OSD07-I02	Cross Platform Digital Rights Management (CP-DRM) System (AF)
OSD07-I03	Anti-Forensics as a Countermeasure to Software Piracy and Reverse Engineering (AF)
OSD07-I04	System Self-Protection and Autonomic Response for Hardware Based Software Protection (AF)
OSD07-I05	Autonomic Kernel Protections to Reduce Attack Susceptibility (AF)
OSD07-I06	Data Base Security mechanisms for Mobile Ad-Hoc Networks (MANETS) (AF)
OSD07-I07	Data Authentication and Dissemination using Watermarking for Net-Centric Operations (AF)
OSD07-I08	Secure Information Assurance in a Global Information Grid Framework (AF)
OSD07-I09	Deep Understanding of Complex High-Assurance Hypervisor Source Code (Navy)
OSD07-I10	High-Assurance Partitioning for Integrated Mixed Criticality Applications (Navy)
OSD07-I11	Distributed, Host-Based Cross Domain Solutions (Navy)

OSD SBIR 07.2 Topic Index

OSD07-CR1 TITLE: Getting the Word Out: Modeling the Propagation of Counter Insurgency Information within a Population

TECHNOLOGY AREAS: Information Systems, Human Systems

OBJECTIVE: Adapt epidemiological models developed for the integrated theoretical and statistical analysis of the influence of individual variation in infectiousness on disease emergence to the prediction of the propagation of counterinsurgency messages within a population.

DESCRIPTION: Marketing research and models tend to focus on maximizing economic return by targeting their message on the mean behavior of the population. Historically insurgents and their active supporters have been a small component of the population (less than 1%). Computer modeling of the spread of viral diseases and comparison against data from actual outbreaks has demonstrated the limitations of models that do not take the full heterogeneity of the host population response and contact rate into account. In addition, Lloyd-Smith et al. addressed this point and identified a highly significant potential role for "superspreaders" in accelerating the spread of the disease over that predicted by a homogeneous model in which parameters based on the population mean are used to describe for the entire population. In the superspreader model relatively few individuals are responsible for most of the transmission. Applied to the dissemination of counterinsurgency messages, such a model if applicable and if the "information superspreaders" in a population can be identified and reached through individual-specific communication strategies, may result in more effective and efficient use of information in counter-insurgency operations. "Viral marketing" used with some effect by small businesses in part exploits this approach. This effort focuses on developing a solid modeling capability for the phenomena and integrating the capability into operations support systems to enhance the effectiveness of military operations.

PHASE I: Evaluate various individual-level epidemiological models for applicability and deployability in field-level command and control systems. Identify key human social, cultural and behavioral parameters that will be required to tune the models to particular areas of current or potential future U.S. military operations. Assess the availability of data to support the assignment of particular values to those parameters noting that models that depend on parameters that are unknowable are not going to be operationally useful. Propose a development path to field a prototype for application in Corps and Theater-level command and control systems.

PHASE II: Develop and demonstrate a prototype system in a lab or simulation environment. Conduct testing to prove feasibility in an operational experiment or training scenario for initial assessment by Systems Commands for integration as an application for higher echelon command and control/operations support systems. Define how forward deployed small teams can obtain information to help define/refine model parameters to more accurately predict the effects of counter-insurgency messages.

PHASE III: Introduce to relevant DoD and USG user activities and commands for usability testing or incorporate as part of the national, theater, Corps and Division-level command and control systems.

DUAL USE: Developing alternate modeling constructs for understanding how ideas foment in populations has implications for Department of Homeland Security and other governmental agencies.

REFERENCES: 1) Lloyd-Smith, J. O. , Schreiber, S. J. , Kopp, P. E. & Getz, W. M. Nature 438, 355–359 (2005).

KEYWORDS: Multicultural, modeling, media, epidemiology

TPOC: Richard Higgins
Phone: 703-602 - 6204
Fax: 703-604-1729
Email: higginsr@iwsp.cttso.gov
2nd TPOC: Chris Dufour
Phone: 703-604-1683

Fax: 703-604-1729
Email: dufourc@iwsp.cttso.gov

OSD07-CR2 TITLE: Virtual Iconic Presence (VIP) for Training and Mission Rehearsal

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Develop artificially intelligent virtual presence molded in the fashion of iconic leaders and activists. VIP will be programmable to a wide range of specific religious, socio-cultural and ethnographic qualities, resulting in a virtual "presence" of a highly influential personality targetable to specific regions, movements or populations. It will be developed to support training and mission rehearsal/experimentation areas within DoD.

DESCRIPTION: Violent extremist movements of the 21st century have become virtual in their proliferation, that is, able to survive virally through franchised adherents rather than doctrinally trained "soldiers for the cause." Architects of these movements – in the fashion of Usama bin Laden for al-Qaeda – remain as spiritual, iconic figureheads, able to inspire hundreds of thousands of supporters through a cult of personality proliferated via virtual means (i.e., videos and statements released through the internet and shared via MySpace, YouTube, and other virtual "communities"). These iconic narrative/influence has a direct, near-term impact on operational and tactical actions of U.S. forces and disrupts strategic planning and goals. To mitigate or remove the impact of these influential virtual messages, it is necessary to develop the capability to train our forces to expect and react appropriately to these events. It is also important to be able to simulate such virtual perturbations/VIPs in support of wargaming and planning exercises in order to develop appropriate courses of action. A VIP fills the role of a personality mirroring those currently countering U.S. national interests. The VIP can furthermore be tailored to specific regional, religious or socio-cultural areas where violent extremism is on the rise. VIPs should be capable of representing multiples ideas or messages based upon an understanding of what generates belief in extremist rhetoric, what influences potential recruits to join violent uprisings. Methods of influence to be modeled may include, but are not limited to: speeches given in chatrooms, message boards and/or email lists; videos of the VIP's virtual façade, slogans and soundbites; podcasts of VIP speeches and/or interviews; interactive educational and learning programs; etc.

PHASE I: Develop artificially intelligent engine for VIP with a base capacity for adaptable human/virtual interactions. Templates for this base engine can be researched in the international gaming community. The metrics for the base engine's success must involve rapid response to programmed stimuli, and adaptation to potentially "game-changing" scenarios within a program, and be relevant/applicable to DoD training and mission rehearsal concepts. The base engine must also be able to draw upon networked sources of programmable information (open source databases, online news feeds, and keyword searches) to remain current.

PHASE II: Develop prototype VIPs using socio-cultural and human behavioral data collected as to create a Usama bin Laden – like personality and its effects / appeal to the global Islamic jihad. Conduct pilot experimentation and testing programs with prototype VIPs within a military training or mission rehearsal exercise.

PHASE III: Using monitored feedback and analysis from Phase II, demonstrate and integrate VIPs into a current military planning, training or mission rehearsal system. Begin operational analysis of additional target regions / movements / personalities in which to develop VIPs.

PRIVATE SECTOR COMMERCIAL POTENTIAL/ DUAL-USE APPLICATIONS: Topic has direct relevance to other U.S. government agencies, as well as the virtual gaming industry and artificial intelligence industries.

KEYWORDS: virtual iconic presence, artificial intelligence, personality simulation, counter-narrative, internet, influence

TPOC: Richard Higgins
Phone: 703-602 - 6204
Fax: 703-604-1729
Email: higginsr@iwsp.cttso.gov
2nd TPOC: Chris Dufour

Phone: 703-604-1683
Fax: 703-604-1729
Email: dufourc@iwsp.cttso.gov

OSD07-CR3 TITLE: Training Leaders and Analysts on Measuring Progress in Conflict Environments (MPICE) Tool

TECHNOLOGY AREAS: Human Systems

OBJECTIVE: Train US military and civilian agency planners and analysts in the proper use and application of the Measuring Progress in Conflict Environments (MPICE) tool and how to maximize its capability to visually interpret and correlate data collected from metrics used to assess progress in complex contingency environments.

DESCRIPTION: Provide a MPICE training support package supporting potential MPICE users that enables planners and analysts to rapidly tailor and apply measures and metrics to measure progress in evolving stability and reconstruction operations by providing a generic set of metrics to be applied to the situation along with a method for gathering data most useful to conduct the assessment. Once gathered this data can be visualized by the MIPICE tool in ways that bring the "to life" by enabling correlation of data from within tasks or across sectors of data. These visualizations do not provide causal relationships between data but should evoke additional analytical questions and promote additional excursions with the data presented that provides planners and analysts the ability to support/reject analytical hypotheses to decision-makers. The challenge is that the sophistication of the tool will require training to apply it and maximize its unique visualization qualities.

The purpose of MPICE program is to establish a system of metrics that will assist in formulating policy, developing strategy and then implementing plans to transform conflict and bring stability to war-torn societies. These metrics provide both a baseline assessment tool for policymakers, planners and analysts to diagnose potential obstacles to stabilization prior to an intervention and an instrument for practitioners to track progress from the point of intervention through stabilization and ultimately to a self-sustaining peace. This metrics system is designed to identify potential sources of continuing violent conflict and instability and to gauge the capacity of indigenous institutions to overcome them. The intention is to enable policymakers to establish realistic goals, bring adequate resources and authorities to bear, focus their efforts strategically, and enhance prospects for attaining an enduring peace.

MPICE spans the security, governance, rule of law, economic and social well-being sectors and addresses strengthening institutional capacity while decreasing drivers of conflict. This framework will be used as the metrics basis for the MPICE analytic tool.

While MPICE will provide a new capability to planners and analysts the total capability of the tool to conduct excursion exercises of test hypotheses are not so evident. The sophistication of the tool would necessitate further training for leaders and analysts alike. Because the MPICE tool is under development and not a program of record there is not plan to develop such a training program. The MPICE program complements on-going efforts to successful accomplishment of US national objectives, not just combat objectives, requires US military planners to plan, prepare and conduct operations across many levels of conflict/warfare. Additionally, emerging MPICE metrics provide indicators, measures, metrics and data collection methods providing critical assessment/analysis to the all levels from policy to tactical. An automated capability is necessary to provide strategic and operational planners with the systematic approach represented in these documents to rapidly categorize and translate USG objectives into sound, executable strategies and tasks.

The envisioned computer-based simulation training tool will provide 8 to 10 scenarios representing complex stability operations environments that allow the user to tailor the generic metric framework to a specific simulation environment, specify resources for strategies and data collection of specific measures over time. We seek a tool with the following features:
1) Ability to train operators to correctly visually interpret and correlate collected data.
2) Accurately render the complexities of the stability operations environment.
3) Include hypotheses based options that allow the user to play different strategies.

4) Have embedded best practices for educating responders in the complexities of stability operations..
5) Exportable (DVD/Web-based) training program with intuitive user interface.
6) Use online learning and updates.
7) Build using open source software architectures
8) DESIRED BUT NOT ABSOLUTE REQUIREMENT – scenario editor to modify scenario variables allowing user to better simulate their specific environment.
9) DESIRED BUT NOT ABSOLUTE REQUIREMENT –includes multiple responder, coalition

PHASE I: Development of a complete concept plan and the design for a prototype system to teach skills required by military and civilian leaders who may be involved in stability operations and provide a working demonstration of the concept. In the concept plan address the following items with respect to phase II requirements:
1) Describe in detail 8 to 10 complex scenarios
2) Describe and illustrate tool(s) under consideration.
3) Model the proposed system configuration with respect to listed requirements.

PHASE II:
1) Build and demonstrate the prototype system.
2) Imbed metrics for training performance assessment.
3) Validate system performance with subject matter experts.
4) Include embedded users manual to be used online.

PHASE III DUAL USE COMMERCIALIZATION: This tool will provide an immediate increased capability throughout the military and civilian communities to measure/monitor the effectiveness of their response to complex contingency operations to include disaster and emergency operations.

KEYWORDS: Computer-based Training, Advanced Learning, Intelligence Tutor, Strategic Planning, Measures and Metrics, Reconstruction, Stabilization, Human, Social, Cultural

TPOC: Dr. Barbara Sotirin
Phone: (202) 761-1415
Fax:
Email: barbara.j.sotirin@us.army.mil

OSD07-CR4 TITLE: Measuring Progress in Conflict Environments (MPICE) Modeling and Simulation Toolchest and Analysts Work Environment

TECHNOLOGY AREAS: Human Systems

OBJECTIVE: Provide US military planners/analysts and their USG Interagency partners with additional capability to measure progress using the Monitoring Progress in Conflict Environments (MPICE) Tool.

DESCRIPTION: Among the most critical Stabilization and Reconstruction Operations (S&RO) challenges the USG interagency faces today are accurate assessments of baseline conditions in conflict environments, and verifiable benchmarks and measurement of progress of S&RO efforts in various places throughout the world.
As Secretary of Defense Rumsfeld stated in October 2003, "We lack the metrics to know if we are winning or losing." Yet, S&RO conducted in complex social and conflict environments are hard to diagnose clearly. Operators in Iraq and Afghanistan recognize they are often measuring outputs rather than outcomes, and support a more rigorous, structured approach to assessing progress. As well, there is a critical stage of conflict transformation where real-time diagnosis of conditions is crucial to stabilizing a region and setting it on the road of improvement so an apriori integrated approach to assessing conditions and monitoring progress is essential.

The US Government is developing a metrics tool though the "Monitoring Progress in Conflict Environments (MPICE)" project. The MPICE tool will provide a new capability to planners and analysts to rapidly apply metrics to tasks developed in support of complex contingency operations. [see references 1, 2 and 3] Additionally, MPICE will provide planners/responders with nascent tools to display and manipulate data in ways helpful to bringing

relevant data "to life" for analysts/leaders. While MPICE provides a systematic framework across 4 sectors, and initial data collection and analysis methodologies, additional work is needed.

1. Extend the MPICE framework to include a "social well-being" sector and investigate the linkages to the 4 sectors that currently exist in the MPICE framework.

2. A key challenge in bringing together the existing and available work in these areas is the development of an approach to fusing different kinds of data. Techniques designed to combine quantitative information, qualitative information, modeling and simulation information, and long-standing country expertise, into a coherent information base that clarifies both defined understanding and key uncertainties and issues need to be developed to integrate the MPICE data. As well analysis methodologies such as content analysis, link analysis, social network analysis, traditional expert analysis, and other methods need to be assessed for applicability and modified for the specific MPICE environment. Information generated external to the S&RO environment in question, internal information, and the variable media selection and amplification of information must be accounted for. While MPICE has the capacity to bring this relevant data to life and offers a comprehensive set of indicators of effectiveness, it does not incorporate state-of-the-art qualitative data analysis techniques, or data integration algorithms that combine results of different data collection methodologies such as content analysis, polls and surveys, physical statistical data and expert opinion.

3. Input, output and outcome measures and metrics are typically distinct. MPICE currently does not substantially and rigorously link the measures of effectiveness focused on "outcomes" to measures of performance or "outputs" of actual activities on-the-ground (miles of roads constructed, number of schools built, number of police trained, etc).

The MPICE program complements on-going efforts to successful accomplishment of US national objectives, not just combat objectives, requires US military planners to plan, prepare and conduct operations across many levels of conflict/warfare. DoD Directive 3000.05 signed 28 November 2005, mandates that: "U.S. military forces shall be prepared to perform all tasks necessary to establish or maintain order when civilians cannot do so." Concerted efforts on the part of USJFCOM and the US Department of State's, Office of the Coordinator for Reconstruction and Stabilization produced two documents of immense value to both US Government and Military Planners - the Draft Planning Framework and the Essential Tasks List. [see references 4 and 5] Together these documents provide a comprehensive approach to establish US policy, strategy and to identify tasks that will accomplish the strategy. This approach is necessary to provide strategic and operational planners with the systematic approach represented in these documents to rapidly categorize and translate USG objectives into sound, executable strategies and tasks.

PHASE I: Extend the MPICE framework to include social well-being goals, indicators and measures and integrate into existing system. Investigate relevant approaches to analyzing and combining quantitative information, qualitative information, modeling and simulation information, and long-standing country expertise, into a coherent information base. Examine the feasibility of applying various approaches to the MPICE system. Provide feedback on how/whether to proceed with Phase II.

PHASE II: Develop specific algorithms for analyzing and integrating the MPICE data into an integrated and comprehensive system for monitoring progress in conflict environments. Integrate these algorithms into the MPICE tool and provide additional useful analysis tools to planners/analysts that link output measures to the MPICE outcome measures.

DUAL USE COMMERCIALIZATION: Has USG-wide and possibly Multinational and International application (United Nations, NATO).

REFERENCES: 1) MPICE METRICS FRAMEWORK FOR ASSESSING CONFLICT TRANSFORMATION AND STABILIZATION; DECEMBER 2006,
ftp://ftp.usace.army.mil/pub/hqusace/SBIR/Metrics%20Framework%20-%20December%202006%20Deliverable%20Final.pdf
2) MPICE Initial Metrics Analysis Tool; December 2006
ftp://ftp.usace.army.mil/pub/hqusace/SBIR/MPICE%20tool%20description%2031%20Dec%202006%20draftsmall.pdf

3) MPICE Literature Review; December 2006
ftp://ftp.usace.army.mil/pub/hqusace/SBIR/MPICE%20Lit%20Review.pdf
4) USG Draft Planning Framework for Reconstruction, Stabilization and Conflict Transformation, USJFCOM J7 Pamphlet, version 1.0, 1 December 2005, http://www.dtic.mil/doctrine/jel/other_pubs/jwfcpam_draft.pdf
5) S/CRS Essential Tasks List, April 2005, http://www.state.gov/documents/organization/53464.pdf

KEYWORDS: Quantitative data analysis, Data fusion, Stabilization, Human, Social, and Cultural measures

TPOC: Dr. Barbara Sotirin
Phone: (202) 761-1415
Fax:
Email: barbara.j.sotirin@us.army.mil

OSD07-CR5 TITLE: Stability Operations Systems Learning Environment

TECHNOLOGY AREAS: Human Systems

OBJECTIVE: Development of an interactive web-based Civil-Military Stability and Reconstruction Operations learning tool for training Federal civilian and military personnel engaged in "whole of government" responses Stability, Security, Transition and Reconstruction (SSTR) operations.

DESCRIPTION: In conditions of state fragility, and in reconstruction/stabilization after conflict or disaster, there are local development needs that go beyond the short-term humanitarian provision of food/shelter/water but are needed well before long-term democratic and economic systems are functioning. Bridging from post-crisis into longer-term development, the international community must be able to respond to local citizens with programs providing food, water, shelter, jobs, education and health options but in ways that are sustainable in the political, economic, social and cultural context of the country and region.

The results of federal SSTR efforts, both interagency and single agency, have been mixed. The experience and training of the SSTR response force, particularly military personnel, is generally inadequate. Cost, time, and manpower considerations prohibit training via traditional means resulting in too many personnel sent into crisis areas without proper training. An automated training tool will greatly improve the opportunity for civilian and military personnel to increase their level of training prior to entering an area of operations (AOR). A web-based training tool will enable personnel to train while actually in an AOR. An interactive web-based tool will allow them to train on the unique requirements of their specific AOR as events unfold on the ground.

A broad range of past operations and lessons learned are available for study in an interactive web-based tool. These include Stability Operations from the post WWII Marshall Plan, analysis of post USSR Soviet Republic and DoD lessons learned from Bosnia, Kosovo, Haiti and more recently Afghanistan and Iraq. The tool will also include the bodies of knowledge from other federal agencies such as the United States Agency for International Development (USAID) and State Department, as well as international organizations such as the United Nations and non-governmental organizations.

This substantial body of development lessons learned from field programs in numerous countries and conditions serve as a basic "menu" of options from which to tailor programs for fragility and post-conflict reconstruction and stabilization. Specialists working in many technical areas such land tenure and property rights, agriculture, workforce development, small and medium enterprise and infrastructure development have developed best practices and lessons learned which need to be adapted for fragility and post-conflict settings. This project will collect, analyze and deliver the extensive development expertise in a systematic manner in order. Made available in an interactive web-based learning tool will assure that relevant best practices are incorporated into SSTR operations as standard operating procedures enabling achievement of operational and strategic objectives.

PHASE I: Identify specific training objectives needed to prepare civilian and military personnel for SSTR operations. Identify 5-8 historical events that illustrate a range of operations in different environments. The results of these operations should reflect success, partial success and failure, ideally all within a single large event. Using

the Political, Economic, Military, Security, Information, and Infrastructure (PMESII) or another similar assessment criteria, describe the conditions of each of the historical events. Describe objectives of the SSTR efforts, the implementation of those efforts, and the results of efforts as the impacted the conditions on the ground. Hypothesize how alternative actions may have created different results. This will enable the user to learn what specific actions or combination of actions may work and not work in a particularly scenario.

PHASE II: Automate the knowledge developed in Phase I into an interactive web-based learning tool. The envisioned computer-based simulation learning tool will provide a systems and life-cycle approach for educating military and civilian operators to invoke comprehensive sustainable solutions. We seek a tool with the following features:

1) Engage the user in a compelling realistic simulation environment.
2) Accurately render the complexities of the stability operations environment.
3) Include hypotheses based options that allow the user to play different strategies.
4) Have embedded best practices for educating responders in the complexities of stability operations.
5) PC-based with intuitive user interface.
6) Use online learning and updates.
7) Build using open source software architectures
8) DESIRED BUT NOT ABSOLUTE REQUIREMENT – scenario editor to modify scenario variables allowing user to better simulate their specific environment
9) DESIRED BUT NOT ABSOLUTE REQUIREMENT –includes multiple responder, coalition responder and multiple threat/spoilers.
10) DESIRED BUT NOT ABSOLUTE REQUIREMENT –includes the capability for approved users to add new scenarios

PHASE III DUAL USE COMMERCIALIZATION: This tool will provide an immediate increased level of knowledge of SSTR operations by civilian and military personnel. The tools further adapted could also be used for training non-governmental personnel involved in relief and humanitarian operations and in an academic environment

REFERENCES: 1) http://www.dtic.mil/whs/directives/corres/html/300005.htm

KEYWORDS: Computer-based Training, Advanced Learning, Intelligence Tutor, Strategic Planning, International Development, Reconstruction, Stabilization, Human, Social, Cultural

TPOC: Dr. Barbara Sotirin
Phone: (202) 761-1415
Fax:
Email: barbara.j.sotirin@us.army.mil

OSD07-I01 TITLE: Information Dissemination Agent (IDA)

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Simplify the document reclassification process by creating seamless integration with the user's native multi-security level desktop environment. Simplify the management of reclassification services by providing a centralized reclassification server for a Service Oriented Architecture environment.

DESCRIPTION: As more information is collected, its ability to be disseminated in a timely manner hinges on the procedure to properly classify the data. Although different agencies can standardize on desktop environments for their users, the document reclassification process varies from site to site since there is no accepted standard. Training on these processes can take from several hours to several days, and they usually are singled out as the bottleneck in the document re-grading procedure. This is usually because these applications are not integrated with standard intra-domain operations of the same type, as such a copy/paste operation between windows in the same classification level, and windows of differing classification levels.

PHASE I: Investigate current multi-level operating system desktop environments, and identify key extension points that would allow for tight integration and transparent operation of a data classification tool (such as copy/paste operation from transfer from one classification window to another). Design and develop an architecture that provides a heterogeneous desktop environment with centralized analysis and review services. These services should assist in assuring that a given document is properly classified, while being non-interruptive with current applications, and can augment their functionality and assist in the reliable human review process. The architecture must address issues of trust in the analysis service, trust in the results, and proper authorization and non-repudiation of classified data. After selecting the appropriate architecture, a proof of concept system can be implemented and demonstrated.

PHASE II: Using the results of Phase I, develop, demonstrate, and validate a prototype system that can be demonstrated using real-world scenarios and appropriate data sets.

PHASE III DUAL USE APPLICATIONS: This technology addresses critical needs of joint and coalition forces in which the improper classification of information can have immediate and potentially devastating negative operational impact. The same can be said in the commercial sector in dealing with "sensitive" information such as individual social security numbers, banking accounts, medical (HIPAA), and other information ripe for identity theft, corporate espionage, etc. This information needs to be classified at the appropriate levels to prevent accidental leakage.

REFERENCES: 1) Classification Guidelines and Distribution Controls ; Executive Order 12958; http://www.usda.gov/da/ocpm/Security%20Guide
/S1class/Classif.htm

KEYWORDS: Accessibility, reclassification, regrader, desktop integration

TPOC: Michael J. Mayhew
Phone: (315) 330-2898
Fax: (315) 330-3913
Email: Michael.Mayhew@rl.af.mil

OSD07-I02 TITLE: Cross Platform Digital Rights Management (CP-DRM) System

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Design and develop a Cross Platform Digital Rights Management (CP-DRM) system which provides a data owner with the ability to control the flow of sensitive digital information even after it has been released. Original Classifying Authorities (OCA) would have options on how to protect their digital information as well as have the ability to track the material when distributed by the receiver.

DESCRIPTION: Controls are needed to enforce protection of sensitive digital information even after the information is released to another party. A cross platform, non-intrusive digital rights management technology can achieve this end with minimal restriction of receiver rights. Therefore, the CP-DRM needs to make the protection element together with the data a self-contained package that will not modify any software or configuration on the receiving system. The technology needs the ability to completely purge the given data from the system without any adverse effect on the rest of the hardware and software. Protection options would range from permission to print, copy, or transfer the information, as well as the number of times to do each. The data owner will also need the ability to set a "time-tolive" of the data for eventual public release or for self-purge of the data on the receiving system. The CP-DRM needs to track distribution of the data after initial release, and document modifications to the original The proposed solution must also address how metadata security mechanisms may be integrated to allow for Multi-Level Security (MLS) information flows. This would provide for pedigree assurance with minimal processing overhead, and enable cross-domain operation.

PHASE I: Perform a study of methods to implement a non-intrusive, platform-independent Digital Rights Management technology. Make recommendations for solution and provide a proof of concept system that addresses at least one of the security issues identified above. Provisions for MLS operation must be shown. Provide prototype demonstration and final report.

PHASE II: Design and architecture requirements documents will be written with emphasis on inter-platform information flow, non-intrusive data protection and sanitization, and auditing of second-hand distribution/modification. A prototype/Engineering Development Model (EDM) would be developed on laboratory systems to demonstrate the feasibility of the design. Participate in lab demonstrations.

PHASE III DUAL USE APPLICATIONS: The final phase would entail the productization of the Cross Platform Digital Rights Management technology for use by the military, homeland security, and the commercial world. The military would use the CP-DRM to protect and track distribution of sensitive and classified material. Commercial sectors can utilize this technology to assure protection of copyrighted material while not interfering with private property rights of the buyer (e.g. music and movie companies).

KEYWORDS: information pedigree, cross-domain, meta-data security, digital rights management

TPOC: Michael J. Mayhew
Phone: (315) 330-2898
Fax: (315) 330-3913
Email: Michael.Mayhew@rl.af.mil

OSD07-I03 TITLE: Anti-Forensics as a Countermeasure to Software Piracy and Reverse Engineering

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Develop innovative anti-forensic techniques that can be used to prevent piracy and reverse engineering of end-node software applications.

DESCRIPTION: The Anti-Tamper--Software Protection Initiative (AT-SPI) Technology Office is charged with preventing piracy, reverse engineering, and malicious alteration of critical national security software and data. AT-SPI has researched, developed, and assessed a wide range of software protection solutions, including those employing software-only as well as hardware-assisted technologies. Software-only protection solutions, while highly adoptable, are susceptible to piracy from logical (i.e. over-the-wire) attacks, where the applications as well as the associated protections are in-band to the attackers. Attackers, who have gained root or administrator access to an end-node, are able to copy the application from the end-node and reverse engineer or alter the software protections in order to execute the application on a host owned by the adversary. Given the relative ease with which one can obtain root or administrator access on a host system, AT-SPI assumes that attackers have the highest level of logical access privilege when developing software protection solutions. AT-SPI is seeking to develop countermeasures to software piracy and reverse engineering using anti-forensic techniques [1]. Anti-forensic technology, such as kernel-mode rootkits [2], has been used by malicious code writers to hide from forensic analysts. In some cases, malware, such as PCI [3] or BIOS rootkits [4] contain an out-of-band component that is difficult to detect. Other anti-forensic techniques include Direct Kernel Object Manipulation (DKOM) [5] and remote execution (rexec) [6], which reduce disk forensic evidence of an attack; and System Management Mode (SMM) [7], which allows a program to execute in a manner that is transparent to the operating system, and hence forensic tools as well. AT-SPI wishes to explore the degree to which these techniques and others can be used to protect software applications from piracy and reverse engineering. AT-SPI is currently performing research and development in kernel-mode software protection as a means to protect applications by making them less accessible (i.e., more out-of-band) to the attackers. However, protection of critical elements of these software protection systems, such as cryptographic keys and algorithms are still a concern due to the fact that these solutions are not completely out-of-band to the attackers. AT-SPI is interested in extending its knowledgebase in the field of anti-forensics (particularly when the technology involves an out-of-band component
or provides a significant deterrent to copying/cloning) and incorporating these techniques in software protection products when appropriate and suitable to the end-users needs. Technology areas of interest (as they apply to their

use in anti-piracy or anti-reverse engineering protection tools) include, but are not limited to, hard-disk or file system anti-forensics [8] [9], volatile memory encryption and out-of-band decryption, BIOS and PCI rootkits, System Management Mode (SMM), remote direct memory access (RDMA) [10], and remote execution. The main focus of this effort is to develop solutions that provide a significant deterrent to attackers wishing to pirate the protected application and their associated protections in order to execute those applications remotely.

PHASE I: 1) Develop an innovative concept for incorporating anti-forensic techniques into a software protection product that will execute on Linux or Windows.
2) Provide design and architecture documents of a prototype tool that demonstrates the feasibility of the concept.
3) Provide a minimal prototype that employs at least one anti-forensic technique.

PHASE II: 1) Based on the results from Phase I, refine and extend the design of the protection tool prototype to a fully functioning solution.
2) Provide test and evaluation results demonstrating the ability of the prototype to defend against both over-the-wire and insider attacks.

PHASE III DUAL-USE COMMERCIALIZATION: Anti-forensic techniques can provide a means to protect critical applications from piracy and reverse engineering. As such, the technology developed under this effort will find use in commercial digital rights management (DRM) products, as well as within the Department of Defense. In addition, the knowledge gained from a thorough understanding of anti-forensic techniques can be used to better detect malicious anti-forensic methods used by our adversaries, malicious insiders, and malware writers.

REFERENCES: 1) Dr. Marcus K. Rogers, “Anti-Forensics,” http://www.cyberforensics.purdue.edu
2) Darren Billy, “Low Down and Dirty, Anti-forensic Rootkits,” Blackhat Asia (Japan) 2006.
3) John Heasman, “Implementing and Detecting a PCI Rootkit,” http://www.nextgenss.com/research/papers/Implementing_And_Detecting_A_PCI_Rootkit.pdf
4) John Heasman, “Implementing and Detecting an ACPI BIOS Rootkit,” Blackhat Europe 2006.
5) Jamie Butler, “DKOM (Direct Kernel Object Manipulation),” Blackhat Europe 2004.
6) Grugq, “FIST! FIST! FIST! Its all in the wrist: Remote Exec,” Phrack Volume 0x0b, Issue 0x3e.
7) Loic Duflot, Daniel Etiemble, and Olivier Grumelard, “Using CPU System Management Mode to Circumvent Operating System Security Functions,” http://www.ssi.gouv.fr/fr/sciences/fichiers/lti/cansecwest2006-duflot-paper.pdf
8) Steven McLeod, “SMART Anti-Forensics.” http://www.noncombatant.org/trove/mcleod-smart-anti-forensics.pdf
9) Irby Thompson and Mathew Monroe, “FragFS: An Advanced Data Hiding Technique,” Blackhat Federal 2006.
10) RDMA Consortium, http://www.rdmaconsortium.org/home

KEYWORDS: Anti-forensics, Software Protection, Kernel-mode, Direct Kernel Object Manipulation (DKOM), Remote Direct Memory Access (RDMA), Rootkits, System Management Mode (SMM), Anti-piracy.

TPOC: David A. Kapp
Phone: (937) 320-9068 x130
Fax: (937) 320-9037
Email: David.Kapp@wpafb.af.mil
2nd TPOC: Christopher Reuter
Phone: (937) 320-9068 x113
Fax: (937) 320-9037
Email: Christopher.reuter@wpafb.af.mil

OSD07-I04 TITLE: System Self-Protection and Autonomic Response for Hardware Based Software Protection

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Advance the effectiveness of software protection techniques and technologies that employ a hardware element by incorporating autonomic characteristics

DESCRIPTION: As currently envisioned, the Global Information Grid (GIG) will consist of about 3 million interconnected computers as well as numerous wireless and mobile components including unattended sensors. If exploited logically or physically, each such device or end-node, having authorized access, may provide an adversary access to trusted DoD systems and information (command, control, and communication systems). Therefore, each end-node must be protected. The Anti-Tamper/Software Protection Initiative (AT-SPI) Technology Office is charged with preventing piracy, reverse engineering, and malicious alteration of critical national security software and data. In order to trust the GIG itself as well as the information shared and processed on the GIG, AT-SPI developed technology protection measures will be essential to establishing and maintaining trust throughout the system, but especially on the individual endnodes. AT-SPI is currently performing research and development in software anti-tamper techniques that employ reconfigurable hardware components to augment software protection systems centered around COTS based computing platforms. Such a protection system involves the coordination between the protected application on the COTS processor and the hardware element of the software protection system. However, this communication can unintentionally provide useful information to an adversary attempting to attack the system[1]. Furthermore, the current solutions under investigation focus primarily on the protection aspects and generally do not consider how to detect attempted tampering nor appropriate responses to triggers. The purpose of this topic is to improve the overall effectiveness of hardware based software protection systems by incorporating autonomic characteristics. Specifically, AT-SPI is interested in investigating (1) protecting the communications between the COTS processor and the hardware protection element, (2) how to detect attempted tamper events, (3) how to differentiate actual tamper events from faults, errors, or intentional device upset designed to deny use of the protected system, and (4) appropriate and graded (intelligent, autonomic[2]) response to sensed triggers (tamper events) including the prevention of denial of service attacks against the protected systems. A successful proposal under this topic should address one or more of the above needs.

PHASE I: 1) Investigate and design an architecture for protected communication and autonomic response between a COTS microprocessor and a trusted reconfigurable hardware component.
2) Provide architectural and design documents of a prototype system that demonstrates the feasibility of the concept.

PHASE II: 1) Based on the results from Phase I, refine and extend the design of the prototype system to a fully functioning protection solution.
2) Provide an analysis demonstrating the robustness of the product to information attacks and appropriate response to such attacks. This should account for attacks involving removal or destruction of the trusted out-of-band hardware component.

PHASE III DUAL-USE COMMERCIALIZATION: Tools and technologies for the protection of high-value software against piracy and reverse engineering and the protection of intellectual property would be marketable in both the DoD and commercial sectors.

REFERENCES: 1) X Zhuang, T Ahang, S Pande, “HIDE: An Infrastructure for Efficiently Protecting Information Leakage on the Address Bus,”
2) www.research.ibm.com/autonomic/

KEYWORDS: Software Protection, PCI card, FPGA, Reconfigurable Computing, Software Anti-tamper, digital forensics

TPOC: Christopher Reuter
Phone: (937) 320-9068 x113
Fax: (937) 320-9037
Email: Christopher.reuter@wpafb.af.mil

2nd TPOC: David A. Kapp
Phone: (937) 320-9068 x130
Fax: (937) 320-9037
Email: David.Kapp@wpafb.af.mil

OSD07-I05 TITLE: Autonomic Kernel Protections to Reduce Attack Susceptibility

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Develop advanced self-monitoring and self-healing techniques for kernel software protection technology.

DESCRIPTION: The Global Information Grid (GIG) requires software security that extends to the end-nodes of the network. Software applications that are vulnerable to malicious alteration, piracy, and reverse engineering can result in the compromise of command, control, and communication channels; as well as piracy and exploitation of central database servers and critical information systems. The Anti-Tamper--Software Protection Initiative (AT-SPI) Technology Office is charged with preventing piracy, reverse engineering, and malicious alteration of critical national security software and data. AT-SPI is currently performing research and development in kernel-mode software protection as a means to protect applications by making them less accessible (i.e., more out-of-band) to the attackers. However, such solutions currently do not address the susceptibility of this technology to over-the-wire or insider attacks, where we define susceptibility as the inherent weaknesses in the protection defenses. AT-SPI is interested in developing autonomic kernel self-monitoring, self-healing, and self-protecting technology as a means to reduce the susceptibility to attacks. In the context of software protection, kernel monitoring involves the static and runtime examination of the application as well as the associated kernel-mode protections. Kernel self-healing involves the diagnosis and repair of those modifications determined to be malicious in order to return to the original unaltered protection system. Kernel self-protecting systems are focused on adapting to the environment and improving the software protection system as necessary. These systems are able to observe their operational environment, detect possible attacks to the system, such as the deployment of reverse engineering tools or unauthorized read/write access, and take action in order to contain the attackers, deploy countermeasures, or adapt to increase the level of protection. Possible approaches include, but are not limited to, kernel runtime process monitoring, where both the kernel protections as well as the kernel monitoring, healing, and protecting components are in the kernel [1]; hypervisor (ring -1) or virtual machine monitoring, detection, and repair of kernel-mode software protections [2]; and remote direct memory access (RMDA) technology, where the monitoring and healing components are on a remote host [3]. Potential solutions could employ software only or hardware-assisted technology.

PHASE I: 1) Develop an innovative concept for an autonomic (i.e. self-monitoring, self-healing, and self-protecting) software protection system that will interoperate with or execute on Linux or Windows.
2) Provide design and architecture documents of a prototype tool that demonstrates the feasibility of the concept.
3) Provide a minimal prototype that demonstrates a self-monitoring, self-healing, or self-protecting technique.

PHASE II: 1) Based on the results from Phase I, refine and extend the design of the autonomic protection tool prototype to a fully functioning solution.
2) Provide test and evaluation results demonstrating a reduced susceptibility of the software protection prototype to attack.

PHASE III DUAL-USE COMMERCIALIZATION: Autonomic software protections will find applicability in forward deployed sensor systems being developed by the DoD. These sensors, which operate in a hostile environment, must be self-aware with regards to their environment in order to adapt and defend against an ever-changing threat. Commercial applications include self-healing systems that can be combined with forensic tools in order to detect, quarantine, or eradicate kernel-level rootkits.

REFERENCES: 1) Julian B. Grizzard, John G. Levine, and Henry L. Owen, “Reestablishing Trust in Compromised Systems Recovering from Rootkits that Trojan the System Call Table,”
http://www.ece.gatech.edu/research/labs/nsa/papers/2004_grizzard_esorics.pdf

2) Julian B. Grizzard, Eric R. Dodson, Gregory J. Conti, John G. Levine, and Henry L. Owen, "Towards a Trusted Immutable Kernel Extension (TIKE) for Self-Healing Systems: a Virtual Machine Approach," http://www.rumint.org/gregconti/publications/20040427_IAW_TIKE_Poster_Extended_Abstract.pdf
3) Florin Sultan, Aniruddha Bohra, Iulian Neamtiu, and Liviu Iftode, "Nonintrusive Remote Healing Using Backdoors," http://citeseer.ist.psu.edu/sultan03nonintrusive.html

KEYWORDS: Autonomic Computing, Software Protection, Self-Healing, Kernel-mode, Remote Direct Memory Access (RDMA), Software Exploitation, Rootkits.

TPOC: David A. Kapp
Phone: (937) 320-9068 x130
Fax: (937) 320-9037
Email: David.Kapp@wpafb.af.mil
2nd TPOC: Christopher Reuter
Phone: (937) 320-9068 x113
Fax: (937) 320-9037
Email: Christopher.reuter@wpafb.af.mil

OSD07-I06 TITLE: Data Base Security mechanisms for Mobile Ad-Hoc Networks (MANETS)

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Perform research into Data Base Security mechanisms for Air Force Mobile Ad-Hoc Networks (MANETS) that are typical of the Air Force's Future Combat System and Warfighter Information Network- Tactical environments. The security solutions formulated would be extremely useful to both the commercial and military worlds. Note that it is anticipated that the security solutions formulated would also be extremely beneficial in the Homeland Defense application by protecting critical computer network infrastructures.

DESCRIPTION: In both the commercial and military world, Data Base security is being recognized as a major emerging problem. It is vital to protect computers and computer networks from hacker and foreign power threats. There are a number of commercially available Data Base Security products that can effectively operate in a static environment, but provide little support for a highly dynamic environment such as MANET. This type of environment can be characterized by:
a. highly dynamic networks with mobile nodes and infrastructure (routing, security, configuration)
b. typically, no concentration points where traffic can be analyzed
c. network addresses do not always reflect location (physical or hierarchical)
d. cannot rely on centralized network or security services
e. intermittent connectivity caused by mobility/ noise
f. normal user behavior not easily characterized due to mobility of networks and dynamic tactical missions
g. forward deployed nodes are susceptible to enemy capture
h. energy, processing, storage constraints
i. bandwidth constraints.
Furthermore, the proposed solution should take into account different levels of classification so data may be shared across multiple security domains. This research will investigate new and innovative approaches for Data Base Security solutions within this highly distributed environment and will support the ability to securely share data across differently-classified secure networks

PHASE I: Perform a study of possible computer and computer network Data Base Security solutions for MANETS. Contractor should also perform a study of what is needed for this project in the encryption area, beyond what is currently commercially available for Personal Digital Assistants (PDAs). Solution must also address classification labeling to enable cross-domain data sharing. A set of alternatives would then be presented to the government. The contractor and the government would make a joint decision on the most promising techniques to pursue in Phase II.

PHASE II: The most promising techniques emerging from the Phase I effort would be further developed and modeled. A performance description or specification would be developed. A prototype software working model

will be delivered.

PHASE III: Military use would include Data Base Security solutions for soldiers who are assigned Wireless Devices in MANET environments. These devices are becoming more prevalent in the military. Commercial uses would include personnel who are assigned Handheld Wireless Devices in such diverse industries as banking, electric power utilities, telephone systems, police and emergency civilian personnel, etc. Note that it is anticipated that the Data Base Security solutions formulated would also be extremely beneficial in the Homeland Defense application by protecting critical computer network infrastructures against outsiders attempting to break into the network.

REFERENCES: 1) www.symantec.com Database Security
2) www.database.about.com/od/security Database Security Issues
3) www.database.ittoolbox.com/topics Database Security
4) www.databasesecurity.com Database Security
5) www.smckearney.com/hncdb/notes/lec.security.pdf Database Security

KEYWORDS: database security, MANET, cross-domain

TPOC: Michael J. Mayhew
Phone: (315) 330-2898
Fax: (315) 330-3913
Email: Michael.Mayhew@rl.af.mil

OSD07-I07 TITLE: Data Authentication and Dissemination using Watermarking for Net-Centric Operations

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: To provide research and development of techniques and deployment strategies for invisible watermarking of digital data for data dissemination and authentication.

DESCRIPTION: Data embedding, in combination with other technologies (encryption, time-stamping, hashing, key management, etc.) can be utilized to ensure that data has not been altered, originates from a trusted source, and/or is delivered only to appropriate systems and personnel. Such binding of metadata within the representation of the cover data itself can establish such properties as the security attributes, pedigree, integrity, and releasability of data. Emphasis for this research is on protocols and system design rather than specific watermarking algorithms. Consider augmenting an application of existing watermarking technology and defining networked ways to use the technology rather than developing additional watermarking algorithms. You are also encouraged to augment/redesign deficiencies in existing algorithms that you identify.

PHASE I: Options for data embedding techniques and content will be proposed, and an analysis of the trade-offs conducted. Strategies and architectures for how elements of the Global Information Grid (GIG) would utilize the watermarks will be proposed. The awardee must provide proof-of-concept demonstration(s) which exhibit the viability of their approaches. The awardee must test the effectiveness of their solution(s) and provide thorough documentation. The awardee will also investigate commercial applications and opportunities.

PHASE II: A full implementation of the data watermarking solution on prototype systems and networks which are representative of the GIG will be domonstrated. All products of the development must be tested, and measurements of validity, effectiveness, and limitations must be recorded. The awardee will meet with DoD accrediting organization(s) for initial consultation on accreditation requirements. The awardee will continue to search out commercial opportunities, consult with users, and verify the deployment strategy for the prototype.

PHASE III DUAL USE APPLICATIONS: Full operational verification and validation of an expanded system will be demonstrated. The awardee will continue to consult with users. The awardee will meet with DoD accrediting organization(s) to chart path(s) for full accreditation of the requisite technologies and system(s). Dual-use applications for the private sector will be fully investigated and developed to the extent commercial investment permits.

REFERENCES: 1) Watermark Evaluation Testbed (WET) Prudue University School of Electrical and Computer Engineering Video and Image Processing Laboratory http://datahiding.net
2) O. Guitart, H. C. Kim, and E. J. Delp, "The Watermark Evaluation Testbed (WET): New Functionalities," Proceedings of the SPIE International Conference on Security and Watermarking of Multimedia Contents, P. W. Wong and E. J. Delp, Eds., January 2006. at http://datahiding.net/about.html.
3) H. C. Kim, and E. J. Delp, "A Reliability Engineering Approach to Digital Watermark Evaluation," Proceedings of the SPIE International Conference on Security and Watermarking of Multimedia Contents, P. W. Wong and E. J. Delp, Eds., January 2006. at: http://datahiding.net/about.html
4) Lossless Data Embedding with File Size Preservation Jessica Fridrich*, Miroslav Goljan, Qing Chen, and Vivek Pathak Department of Electrical and Computer Engineering SUNY Binghamton, Binghamton, NY 13902-6000, USA

KEYWORDS: Watermarking, Data Embedding, Data Authentication, Imagery, Audio, Video, Information Assurance, Key Management, Time-stamping, Encryption, Hashing

TPOC: Chad Heitzenrater
Phone: 315-330-2575
Fax: 315-330-2022
Email: Chad.Heitzenrater@rl.af.mil

OSD07-I08 TITLE: Secure Information Assurance in a Global Information Grid Framework

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Develop an enterprise-wide software solution to classification regrading that facilitates secure information assurance in a Global Information Grid framework.

DESCRIPTION: Ensuring the security of the net-centric capabilities of the GIG is necessary for information assurance. Within a distributed network that contains many edge nodes, trust and robustness must be distributed across the networks into nodes that were once isolated within on-site secure networks. The resulting dynamic security schemes must manage cross-domain data access and dissemination. Within the dynamic operational environment, as mission needs change, documents necessarily become reclassified. This process needs to be automated, enabling the appropriate personnel to acquire access to the data without additional personnel in the loop. In addition, with the increased use of joint, allied, and coalition modes of warfare, the GIG requires a means for rapid, decentralized determination of “need to know.” The proposed solution should address improvements to existing document classification techniques or new approaches to the problem. Organizations must often perform manual document summarization in order to make available documents of less sensitive nature, for instance for use in joint, allied, and coalition operations. Proposed solutions should also address automated approaches to this task.

PHASE I: Develop and architect a distributed approach to dynamically reclassifying documents across multiple domains, and to providing documents of lower classification levels to users of limited access permissions in a dynamic, operational environment. In addition, describe in detail the methods for testing and evaluating the effectiveness of the proposed technical approach.

PHASE II: Develop and implement a prototype system based on the Phase I effort. In addition, test and evaluate the accuracy, robustness and scalability of the resulting software, as well as the effectiveness of the software in distributed information environments such as the GIG. These prototypes should be made available to the responsible COTR for testing in an operational environment.

PHASE III DUAL USE APPLICATIONS: The need to rapidly and securely share information is an intelligence community-wide problem. In addition, commercial organizations face the same need for software to provide dynamic, enterprise-wide secure data management. For instance, companies must balance the need for visibility with the need to secure intellectual property. The proposed solution must address the need for distributed software to automate the task of classification regrading within the intelligence community as well as the private sector.

REFERENCES: 1) “Classification Management”. https://dssaots.dss.mil/bisuappdf/bisuaplesson4.pdf
2) “Department of Defense Contract Security Classification Specification (DD Form 254)”.
3) DoD 5200.1-H, "Department of Defense Handbook for Writing Security Classification Guidance," http://www.dtic.mil/whs/directives/corres/text/p52001h.txt
4) Sabastiani, F. Machine learning in automated text categorization. ACM Computing Surveys, 34(1), 2002.
KEYWORDS: natural language processing (NLP), automated classification regrading

TPOC: Mr. Craig S. Anken
Phone: 315-330-4833
Fax: 315-330-8069
Email: Craig.anken@rl.af.mil

OSD07-I09 TITLE: Deep Understanding of Complex High-Assurance Hypervisor Source Code

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Develop innovative static analysis tools and techniques for deep understanding, refactoring, and increasing the robustness of high-assurance hypervisors used to protect host execution environments in a GIGNCES architecture.

DESCRIPTION: The many GIG-NCES applications of hypervisor technology all require that the hypervisor be highly robust — otherwise, any reliability and security needs will be undermined. Recently, open-source projects have made hypervisor technology widely available. Existing implementations are not designed with high robustness [1] or evaluation [2] in mind. The existing implementations lack: 1) high-robustness protection features, 2) required internal structure, and 3) evidence for security evaluation. Existing hypervisors are built without the use of formal methods, and use highly efficient languages that defy subsequent application of formal methods. Other tools and techniques that work directly with the existing source code must be used to obtain the deep understanding needed to address the three deficiencies. Existing source code analysis tools cannot provide this for hypervisor source code. Hypervisor source code involves many interrelationships, the fundamental structures are duplicated between the hypervisor itself and the guest operating systems, and the virtualization logic that maps between the hypervisor functions and the guest functions is complex as well. Existing static analysis tools that can fully parse hypervisor source code support only shallow understanding, such as a catalog of symbols used. Existing deep understanding static analysis tools cannot fully parse the complex source. What is needed is a deep understanding tool or technique that can fully parse complex hypervisor source code.

PHASE I: Describe and develop creative methods, techniques and tools for deep understanding of hypervisor source code through static analysis. The tools must provide deep understanding, including static backward, forward and sectioned program slicing, for source code comprising interrelated use of preprocessor languages, compiler pragmas, intermediate level languages such as C, and assembler language. The tools must provide deep understanding of highly concurrent designs, complex virtualization logic, and source code that directly manipulates hardware. The tools must significantly lower the cost of increasing robustness and constructing evaluation evidence for high-assurance hypervisors. This phase will develop an initial prototype that demonstrates the feasibility of fully parsing complex source code from an open source hypervisor implementation.

PHASE II: Develop, implement and validate an advanced prototype deep understanding tool based on the techniques used to build the initial prototype of Phase I. The prototypes should be sufficiently detailed to evaluate their effectiveness by increasing the robustness and enhancing the internal structure of an example open source hypervisor and constructing a corresponding high-assurance evidence package for it.

PHASE III DUAL USE APPLICATIONS: Military application: the work funded under this effort would dramatically lower the cost of developing and certifying low level system code such as that used on embedded weapons systems and other key components of a GIG-NCES architecture. These components would include embedded cryptographic devices, high-assurance trusted platform modules, embedded cyber-defense modules,

firewalls, and downgraders. Commercial application: the results funded under this effort have extensive commercial applications, especially in certifying devices in the aerospace and medical fields.

REFERENCES: 1) DOD Instruction 8500.2, February 6, 2003, Information Assurance (IA) Implementation
2) Common Criteria for Information Technology Security Evaluation, Ver. 3.2, June 2005
3) Mark Weiser. Program slicing. Proceedings of the 5th International Conference on Software Engineering, pages 439–449, IEEE Computer Society Press, March 1981.
4) Frank Tip. A survey of program slicing techniques. Journal of Programming Languages, 3(3), September 1995.

KEYWORDS: Hypervisor, robustness, static analysis, high-assurance

TPOC: John McDermott
Phone: 202-404-8301
Fax: 202-404-7942
Email: John.McDermott@NRL.Navy.mil

OSD07-I10 TITLE: High-Assurance Partitioning for Integrated Mixed Criticality Applications

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Develop a real-time, fault-tolerant, high assurance environment to host mixed criticality, mixed security, and mixed domain applications on shared hardware resources to increase functionality and lower size/weight/power costs over current solutions.

DESCRIPTION: Integration of avionics and mission applications reduces their size/weight/power requirements to enable increased range, additional payload capacity, and reduced logistics footprint and costs. Integration complexities, however, can increase costs especially if mixed-criticality applications (e.g., safety critical, mission critical, non critical) are hosted on the same resource because every application, regardless of criticality, must be certified (tested) to the level required by the highest criticality application hosted on the resource. This is tremendously expensive for complex systems such as Unmanned Autonomous Systems (UAS) which serve as remote sensing and increasingly as target illumination and weapons platforms.

As a partial solution, commercial avionics standards, such as ARINC 653, were developed to provide some time and space guarantees, permitting mixed criticality without the same increased testing costs. Developing applications for these constrained operating environments, however, carries additional burdens. Code developed for Linux or other operating systems must be ported and separately maintained. In addition, these commercial applications and avionics solutions do not provide high assurance operations in the presence of military threats; they were designed to provide integrity and availability in a benign commercial world. This topic solicits a time, space, and resource partitioned real-time, fault-tolerant, high assurance operating environment to host mixed criticality, mixed security, applications on shared hardware resources. The successful approach will support different operating systems in the different partitions and demonstrate a path for existing applications to be efficiently ported into this environment. A successful approach will be built using open technology. To achieve the size/weight/power advantages of integration, while maintaining cost advantages of federated architecture development, the underlying architecture must provide domain-specific properties to the different applications. For instance, controls applications often require real-time behavior, where real-time in this context implies provable (or high confidence in) bounds on performance, e.g., guaranteed latencies, processing time, jitter. Similarly, safety or mission-critical operations often require fault-tolerant guarantees, including highly available data, communications, and processing, and integrity guarantees for appropriate fault scenarios. Voting, redundancy, command/monitor, master/shadow, and other hot sparing techniques traditionally satisfy these needs; doing the equivalent in the envisioned environment will need new design, development, verification, and validation techniques. Hardware implications must be understood and quantified.

Some applications hosted on these systems might be at the other end of the spectrum. For instance, remotely operated sensing and reconnaissance platforms requiring varying degrees of autonomy can be non real-time, and can have fairly broad envelopes of memory and computing requirements. The interactions with, and constraints on the environment might enable new capability in these autonomous systems. Similarly, these autonomous systems hosted on the environment could potentially corrupt or violate underlying principles. The environment will need to provide sufficient time, space, and resource partitioning guarantees to permit hosting autonomous systems on otherwise high assurance, real-time, mission critical systems.

PHASE I: Develop requirements and evaluation metrics for the envisioned real-time, fault-tolerant, high assurance environment and assess its technical feasibility. The metrics must include cost effective integration of mixed criticality applications implemented on different operating systems to operate on a single hardware resource. Document approaches for addressing real world issues, including mixed criticality, integrated systems including development, certification, deployment, maintenance, and operation. Assess the feasibility of building the envisioned system. If the assessment is favorable, then produce a plan to implement the environment. Such a plan should document the development phases, the achievements and corresponding tasks for each phase, and estimates for the allocation of resources to given tasks. Produce a schedule which shows how the work will be realistically completed within the schedule and financial constraints imposed by the contract.

PHASE II: Build upon the Phase I results to develop and test the real-time, fault-tolerant, high assurance environment for a specific target application. Demonstrate hosting mixed criticality and mixed security applications on shared hardware resources, and evaluate against metrics developed in Phase I.

PHASE III DUAL USE APPLICATIONS: Work with military and commercial vendors to deploy the environment on a real world application. These can include military platforms and dual use applications. Dual use applications include systems such as commercial avionics, SCADA systems, and embedded medical devices. For example, as Unmanned Air Systems (UASs) become more prevalent, they will need to need to share access to National Airspace System (NAS) and operate within FAA or other regulatory constraints.

REFERENCES: 1) J McDermott and M Kang, "An Open-Source High-Robustness Virtual Machine Monitor," Naval Research
Laboratory, http://acsa-admin.org/2006/wip/ACSAC-WiP06-06-McDermott-WIP0.pdf
2) ARINC Specification 653P1-2 Avionics Application Software Standard Interface, Part 1 - Required Services
3) J Rushby, "A Comparison of Bus Architectures for Safety-Critical Embedded Systems," Sept 2001, SRI International, Menlo Park, CA
4) T Levin, C Irvine, T Nguyen, "A Least Privilege Model for Static Separation Kernels", Oct 2004, http://cisr.nps.navy.mil/downloads/nps_cs_05_003.pdf

KEYWORDS: Mixed Criticality Systems, High Assurance, Time and Space Partitioning,

TPOC: John McDermott
Phone: 202-404-8301
Fax: 202-404-7942
Email: John.McDermott@NRL.Navy.mil

OSD07-I11 TITLE: Distributed, Host-Based Cross Domain Solutions

TECHNOLOGY AREAS: Information Systems

OBJECTIVE: Develop an architecture and framework for a flexible, high assurance cross-domain solution (CDS) that can secure the flow of information between security domains on a multi-domain host.

DESCRIPTION: Navy missions are increasingly being performed as part of a joint-service or coalition of communities. Net-centric warfare in such an environment induces a requirement that personnel be able to efficiently share information between security domains in a manner consistent with the security policies of all the domains involved in the information exchange. Traditionally guards residing on the perimeters of single domain networks

have provided cross-domain security. However, these guard solutions do not provide an adequate cross-domain solution for the evolving hypervisor-based multi-domain hosts [1]. There is a need for a CDS solution that can be distributed to each of the hosts.

Although hypervisors provide an obvious way to isolate the CDS functionality in a separate partition, several problems must be addressed to make such a solution practical. First, cross-domain sharing policies will differ depending on membership in the coalition and its mission. Thus, the CDS must provide a flexible framework on each host so that a new policy can be implemented quickly with little or no recertification effort and in a way that is easily understood and managed by the system administrators and policy authors. Second, the definition of the policy must be centrally controlled and the appropriate portions of the policy securely distributed to each of the CDS partitions on the various hosts. Moreover, the per host policy implementation framework and policy control and distribution must form a single system that can satisfy the high assurance requirements associated with EAL 6 or 7 of the Common Criteria.

PHASE I: Develop the requirements and architecture for a distributed, host-based CDS that supports the EAL 6 assurance requirements. Develop an initial prototype that demonstrates the functional behavior of the system and shows how the system supports the rapid definition and dissemination of CDS policy for coalitions. Prepare a draft Security Target [2] for the system that clearly identifies the assumptions made regarding the Security Functional Requirements and Security Assurance Requirements satisfied by the underlying hypervisor platform.

PHASE II: Develop an operational prototype consistent with the needs of FORCENET and the Global Information Grid and demonstrate in the context of a relevant application. Prepare an assurance plan consistent with the Composition Assurance Level – C (CAP – C) requirements of the Common Criteria.

PHASE III DUAL USE APPLICATIONS: Work with DoD contractors to develop and deploy an operational version of the distributed, host-based CDS. Work with commercial security vendors to transition the technology to commercial products. Many commercial environments are inherently cross-domain. Many manufacturing organizations and critical infrastructure providers are beginning to connect their IT domains with mission or life critical processing control domains. Many other organizations are engaging in cross-federation sharing of selected information. In all these cases there are employees who need access to multiple domains and who need to transfer information between these domains. A cost-effective, distributed CDS on a multi-domain workstation would enable them to use their computing resources and their time more efficiently, and would ensure the timely transmission of critical information to the appropriate entities in all domains.

REFERENCES: 1) Paul A. Karger. Multi-Level Security Requirements for Hypervisors. ACSAC 2005 - Annual Computer Security Applications Conference. Applied Computer Security Associates (ACSA) and IEEE Computer Society, August 2005.
2) Common Criteria for Information Technology Security Evaluation, September, 2006, (www.commoncriteriaportal.org/public/files/)

KEYWORDS: Coalition Communications; Cross Domain Solution, High Assurance, Hypervisor

TPOC: John McDermott
Phone: 202-404-8301
Fax: 202-404-7942
Email: John.McDermott@NRL.Navy.mil