

NATIONAL CYBER RANGE PROPOSERS' DAY

Michael VanPutte, Ph.D.
Lieutenant Colonel, U.S. Army

Program Manager
DARPA/Strategic Technology Office
baa08-43@darpa.mil





Administration



2

- This Workshop is *unclassified*.
 - There are no classified facilities in this building
- PLEASE silence your cell phones and PDAs
- Q&A Cards in your conference packet
 - Turn cards in before lunch; I'll answer some questions after lunch
 - Questions/Answers will be posted to the DARPA Program Website
- The definitive requirements, objectives, metrics for the NCR Program are in:
 - Broad Agency Announcement (BAA)
 - Classified Addendum
 - Security Classification Guide (SCG)
- Those documents supersede anything stated at the Proposers' Day
 - DARPA may publish a clarifying addendum after the Proposers Day



Goal



- **Establish and operate the Nation's premier cyber test facility**
 - **Unbiased, quantitative and qualitative assessment of information assurance and survivability tools in a representative network environment**
 - **Replicate complex, large-scale, heterogeneous networks & users in current & future DoD weapon systems and operations**
 - **Multiple, independent, simultaneous experiments**
 - **Realistic testing of Internet/GIG scale research**
 - **Develop and deploy revolutionary cyber testing capabilities**
 - **Enable the use of the scientific method for rigorous cyber testing**



Providing the environment for others to solve the Nation's cyber challenges



Why



- Over the ages scientific progress has been held back by the ability to make measurements at the necessary level of the environment for which the scientific research was being done.
 - Telescopes, microscopes, particle accelerators, etc.
- The Cyber Test range is the measurement capability for cyber research in both classified and unclassified environments. Without it, any research will be done in darkness and only stumble accidentally into the light.

Enable a revolution in the Nation's ability to conduct cyber operations



What Are We Going To Test?



- **The Nation's cyber R&D initiatives may include...**
 - **Host security systems**
 - **Modify/replace operating systems, kernels, endpoint components**
 - **Wholesale replacement of information technologies**
 - **Local area network (LAN) security tools and suites**
 - **May modify/replace traditional network operating systems, devices and architectures**
 - **Wide-area-network (WAN) systems**
 - **Operate on bandwidths not commercially available today,**
 - **Modify/replace traditional network device operating systems, devices and architectures.**
 - **Tactical networks**
 - **Mobile ad hoc networks, maritime systems, etc.**
 - **New protocols**
 - **Replace portions or the entirety of today's protocol stacks.**



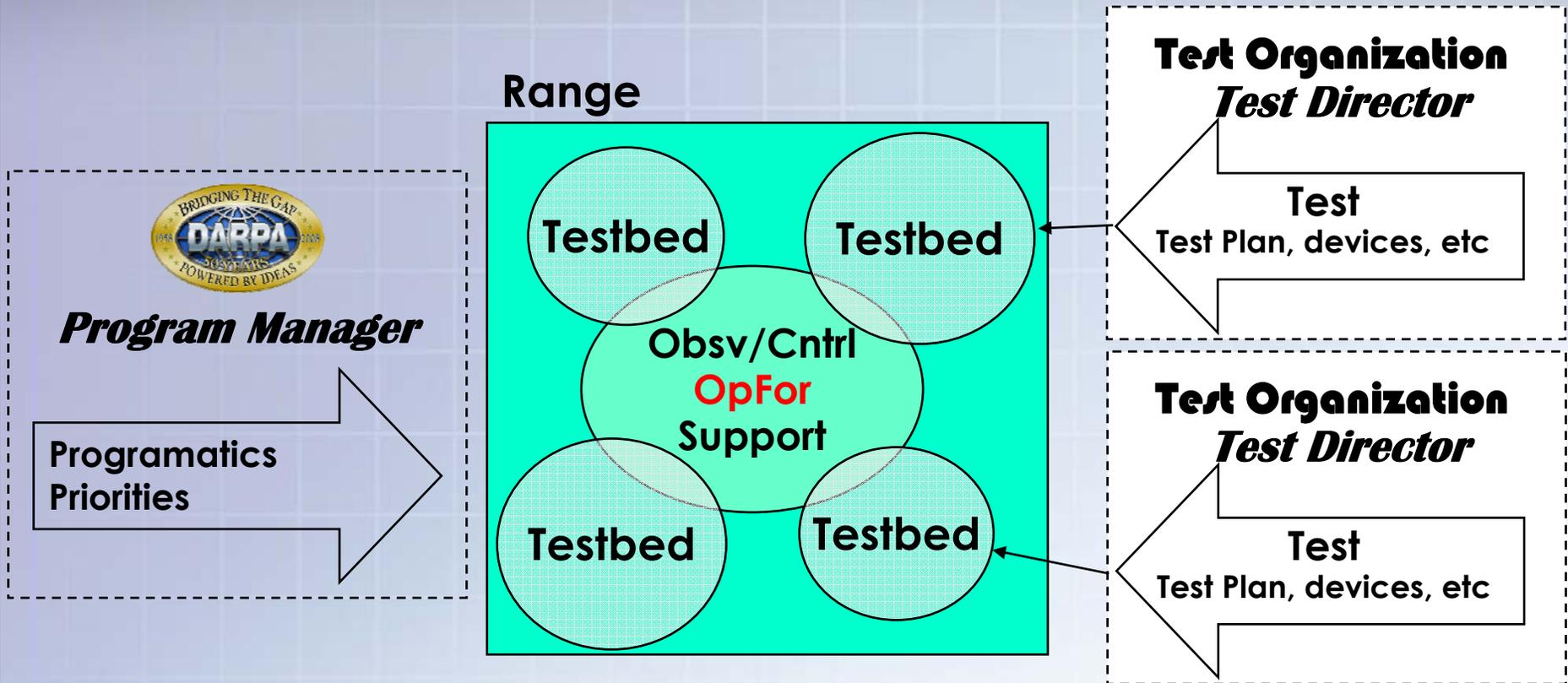
The NCR is not...



- **A bunch of computers connected together**
 - We're going to advance the state of the art in automated test ranges
 - Range Management and Test Management
 - Responsive Traffic Generators (human emulation)
 - Replicated hosts
- **Testbed for existing commercial products**
 - While we may install commercial tools – the purpose is to test revolutionary cyber research programs
- **Demonstration/training site to improve/operationalize existing capabilities**
 - There are other government facilities that do this.

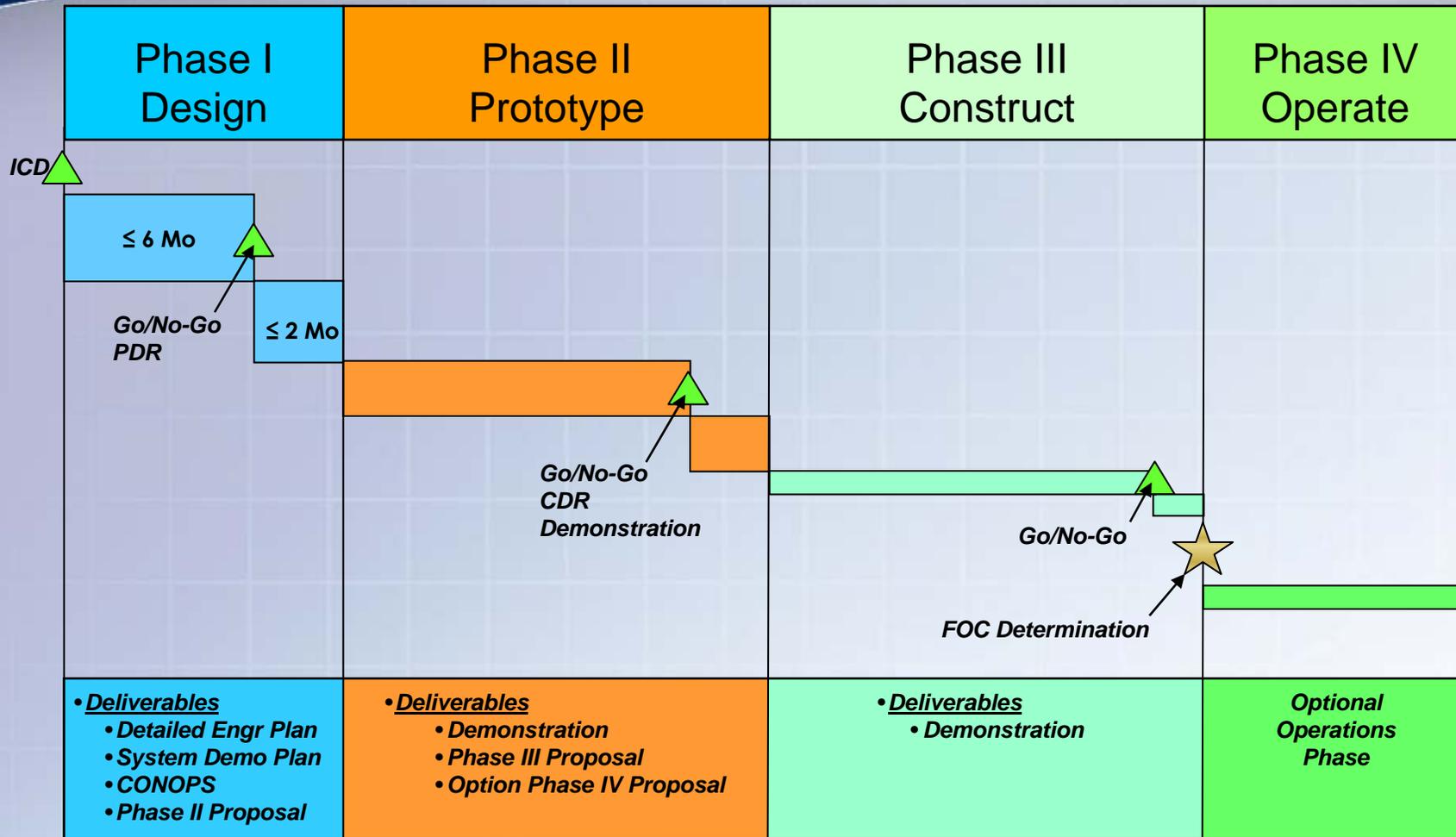


Program Vision





Program Timeline



ICD - Initial Conceptual Design
 CDR - Critical Design Review

PDR - Preliminary Design Review
 FOC - Full Operational Capability



Period Of Performance



- **Phase I**
 - DARPA has not established a funding objective for Phase I
 - DARPA does not expect Phase I to exceed 6 months + 2 months for Final Report preparation.
- **Phase II, III, IV**
 - DARPA has not established a funding objective or a period of performance for Phases II-IV.
 - Performer will propose to meet the minimum Phase II-IV objectives.
- **The government intends to make an award decision based on best value.**



Programmatics



IMPORTANT NOTE

The Government's obligation under this announcement and resulting contract award is contingent upon the availability of FY09 funds which as of the date of publication of this BAA have NOT been Authorized or Appropriated by the U. S. Congress.

In order to expedite the progress of providing this capability, DARPA has published the BAA in FY08 with the expectation that award will be made promptly if FY09 resources are approved and available.

- The BAA is for the National Cyber Range Program
 - Funding for Phase I only
 - Subsequent phases will be limited to successful performers and availability of funds
 - *Once we award the contract the performer will be funded for Phase I; and eligible for Phases II - IV funding based on performance*
 - There is no intent to release a solicitation for subsequent phases



Programmatics (continued)



- **The program solicitation:**

- **Unclassified BAA DARPA-BAA-08-43**
- **Classified Addendum to DARPA-BAA-08-43**
- **Security Classification Guide (DARPA-CG-502)**



Q: "How do I get these?"

A: See BAA Sec 6.1.

- **Proposals must address all requirements to qualify for review/consideration**

- *The government will solidify Phase II-IV requirements on:*

- *Phase I Kick-Off meeting + 30 days (~Contract + 60 days)*

- **Proposers must propose a complete, integrated system.**

- **DARPA will not act as the integrator**
- **DARPA will reject proposals for components of the NCR**



Programatics (continued)



- **Teaming**
 - Collaboration and teaming is strongly encouraged
 - Teaming website referenced in the BAA
 - Proposers may participate on multiple teams
 - DARPA will only accept 1 proposal per prime contractor/team lead.
 - Work toward a common objective
 - Have a unified management structure & single, designated POC authorized to communicate on behalf of all team members

- **Classified participation is restricted to U.S. firms only**
 - Foreign-Owned US Companies:
 - A National Interest Determination (NID) is required when a foreign owned company requires access to classified information. NISPOM Section 2-303c.2
 - Prime contractors should petition DARPA for the NID on their behalf

- **NCR must operate to Top Secret/Special Compartmentalized Information/ Special Access Program classification (TS/SCI/SAP)**

NATIONAL CYBER RANGE PROPOSERS' DAY

**Phase I
Design**





Phase I – Design Phase Overview



- **Provided that FY09 funds are authorized and appropriated:**
 - DARPA expects to fund multiple, competing performer teams for simultaneous execution of Phase I
- **Performers will have at most 6 months:**
 - Refine the performer's NCR ICD (delivered in the Proposal)
 - Detailed Engineering Plan and System Demonstration Plan
 - Develop Concepts of Operations (CONOPS)
 - Phase II Proposal
- **By the end of Phase I convince DARPA that plans, CONOPS, and Phase II proposal**
 - Are feasible with acceptable risk
 - Are a credible/affordable approach to reduce system risk w/in schedule
 - That continuation to Phase II is warranted



Phase I - Deliverables



- **Preliminary Design Review**
 - **System Demonstration Plan**
 - How do you intend to execute the Phase II CDR Demonstration?
 - **Detailed Engineering Plan**
 - How do you intend to meet the Phase III objectives?
 - **Concept of Operations (CONOPS)**
 - How will your Phase III NCR operate?
- **Proposal to build a prototype NCR must demonstrate the ability to:**
 - Meet all Phase II Program Objectives
 - Conduct the Phase II CDR
 - Conduct the Phase II Demonstration

“The PDR should strike a reasonable balance between the performer’s agile practices utilized in the program and the formality of a more conventional PDR that meets the intent of more rigorous existing or expired standards (e.g. MIL-STD-1521B). DARPA will assess the performers against the Go/No-Go Metrics established in Section 3.3.1.”



Phase I - Go/No - Go Metrics



- **To be considered for selection for Phase II:**
 - **Preliminary Design Review (PDR) must demonstrate the feasibility to meet the Phase III Program Objectives :**
 - **Detailed Engineering Plan**
 - Is sufficient and ready to be put under configuration control
 - **System Demonstration Plan fully**
 - Defines how the performer will complete the detailed design, development, fabrication and verification testing of its demonstrator system in Phase II
 - **CONOPS**
 - Clearly explains how the envisioned Phase III NCR will operate, and that this vision meets all Phase III objectives
 - **Critical path analysis**
 - Is complete in a software tracking tool
 - **Phase II Proposal**
 - **Must meet the criteria specified in BAA Sec 6.3 (proposal format)**

NATIONAL CYBER RANGE PROPOSERS' DAY

Phase II

Prototype and Demonstration





Phase II – Prototype Overview



- **Contingent on authorization/appropriation of program funding**
DARPA may fund multiple, competing performers for Phase II to simultaneously build competing prototype NCR ranges
 - Assessment of the ability of each contractor team to successfully achieve program goals by program end
 - Technical merits of the work performed
 - Overall program budget constraints.
- **The primary objectives of Phase II:**
 - Refine/execute the performer's engineering plan and demonstration plan
 - Deliver a prototype NCR.
- **By the end of Phase II, convince the government that:**
 - Components/integrated system performs as stated & Go/No-Go metrics;
 - Plan represents a credible/affordable approach to reduce system risk within schedule;
 - Continuation to Phase III is warranted.



Phase II - Deliverables



- **Critical Design Review (CDR)**
 - Update and complete designs
 - Develop a prototype range
- **Demonstrate prototype NCR**
 - Proposer defines the scale of the Phase II range
 - Prototype range is expected to be significantly smaller than the final NCR
 - Scale necessary to:
 - Meet the Phase II Prototype Objectives
 - Demonstrate current capabilities for the CDR
- **Proposal for Phase III, with an option for Phase IV**



Phase II – Prototype Demonstration Objectives



- Deploy 2 different host node recipes
- Create new recipes
- Rapid testbed reconstitution
- Test management suite
- Time synchronization and auditing
- Data collection tools to include packet capture, event log collection, malware event collection, and automated attacks.
- Traffic generation system to include but not limited to HTTP traffic, incoming/outgoing email, port scanning, automated attacks.
- Responsive traffic generators that drive office software products, browsers, media players, and email clients
- Replicated inter-enclave communication channels on a single test
- Aggregating all nodes and executing one large test/testbed
- Dynamically freeing resources from tests and reassigning them to other existing or new tests



Phase II - Go/No-Go



- DARPA will conduct a CDR level evaluation of the plans/prototype, and a number of test scenarios.

**The Go/No-Go Metrics for Phases II – IV are notional and may change.
The government will solidify the requirements at Kick-Off + 30 days**

- Proposals for Phase III will only be accepted by Phase II performers
- To be considered for selection for Phase III:
 - Provide a CDR-level Detailed Engineering Plan and prototype
 - Demonstrate CDR-level capabilities
 - Demonstrate proposed means to meet Phase III scale & objectives.
 - On the prototype range, demonstrate all program Objectives in Sec 2.2.1 and:
 1. Reconstitute test nodes within 30 minutes.
 2. Reconfigure the range using recipes and configuration files within 2 hours.
 3. Create a 100-node test from DARPA-provided specifications (network diagrams, configuration files, etc) within 6 hours.
 4. Perform time synchronization across all machines to within 10 milliseconds (ms).
 5. Provide quantitative metrics for traffic simulation, user replication, range instrumentation, and range verification of tools.
 - Phase III/IV Proposals must meet the criteria specified in Sec 6.3.

NATIONAL CYBER RANGE PROPOSERS' DAY

Phase III





Phase III - Construct



- Based on the progress and technical maturity achieved during Phase II, DARPA may select a *single* performer for Phase III
- Phase III will result in full-scale NCR development
- Phase III will end with full-scale evaluation of the NCR and operational testing of cyber research programs
- Full Operational Capability (FOC)
 - If the performer achieves the Phase III Go/No-Go criteria



Phase III - Deliverables



- **NCR Core - Recipes & automated test/resource management**
 - **2.3.1.4. Node Replication – endpoints and routing infrastructure**
 - **2.3.1.5. Recipes**
 - A set of instructions that describes the configuration of a node that may include hardware, firmware, metadata, user data, and software (operating system, applications, services, etc).
 - A recipe may be an electronic image of a configured node.
 - **2.3.1.6. Network Technologies and Support**
 - Wired and wireless recipes
 - **2.3.1.7. Protocols and Services**
 - Current and future across the stack
 - **2.3.1.8. Scalability.**
 - **2.3.2. Range Management**
 - “How will the NCR Proposer manage the NCR resources?”

Replication - Any means to reproduce a capability – including but not limited to physical duplication, emulation, virtualization, and simulation.



Phase III - Deliverables



- **2.3.3. Test Management**
 - “What is the Test Director’s interface to the NCR?”

- **2.3.4. Transparency**
 - 2.3.4.1. Instrumented - ground truth of what occurred during tests
 - 2.3.4.2. Observer/Controller - Qualified, on-site evaluation teams

- **2.3.5. Qualified, On-Site Support Team**

- **2.3.9. Encapsulation**



Phase III - Deliverables



- **2.3.6.1. Oppositional Forces (OpFor)**
- **2.3.6.2. Team Integration**
- **2.3.6.3. Traffic Generators**
- **2.3.6.4. Responsive Traffic Generators and Program Activators**
- **2.3.7.1. Extend the NCR**
- **2.3.7.2. Realistic Node Replication**
- **2.3.8. Time Dilation/Contraction**



Phase III - Go/No-Go Metrics



The Go/No-Go Metrics for Phase II – IV are notional and may change. The government will solidify the requirements after the Phase I Kick-Off meeting

- Testing may include multiple, simultaneous tests of research technologies, architectures, and operational plans.



Phase III - Go/No-Go Metrics NCR Full Operational Capability (FOC)



- **Demonstrate all Phase III program Objectives**
- **Successfully demonstrate NCR end-to-end Objectives**
 - **Creating, loading, operating, de-allocating several National tests:**
 - Reconstitute test nodes w/in 15 minutes
 - Reconfigure the range using recipes and configuration files w/in 1 hour
 - Create a 10,000-node test from DARPA-provided requirements (network diagrams and configuration files) w/in 2 hours
 - Perform time synchronization across all machines to w/in 1 millisecond (ms)
 - W/in 4 hours, create logical instantiations of DARPA-provided physical native machine to the interrupt level, including chipset and peripheral cards, and score within 10% of native machine benchmarks
 - Satisfactorily close all Test Director initiated trouble tickets within 4 hours
 - Replicated networks perform w/in 10% of a physical network on DARPA-provided benchmarks
 - Demonstrate human-level behavior on 80% of traffic generated events
 - Increase/decrease test time by at least 25% w/ no changes to test results

NATIONAL CYBER RANGE PROPOSERS' DAY

Phase IV Operations





Phase IV – Operate the NCR



- **Conduct cyber testing on programs of national interest**
- **At Government request, and contingent upon successful negotiation of a mutually agreeable contract between the Government and the performer in accordance with all applicable law (including the Competition in Contract Act, 10 USC 2304), the performer should be prepared to operate the NCR as a national research and development resource**
- **Phase IV proposal:**
 - 12 month period of performance
 - An additional 12 month period of performance option exercisable at the sole discretion of the Government

NATIONAL CYBER RANGE PROPOSERS' DAY

Submissions





Proposals



The decision to continue to Phases II – IV is based upon the performer's successful completion of the previous phases and funds availability

- The government will solidify Phase II-IV requirements on:
 - Phase I Kick-Off meeting + 30 days
- Proposal are due to DARPA NLT 4:00 PM Eastern on 30 June 2008 in order to be considered during the initial round of selection
- Include enough detail to permit DARPA to make an informed decision **that the proposer** has the technical knowledge, team, and understanding of government objectives to *develop a full Phase III National Cyber Range*
- Phase II/III tentative schedule/cost rough order of magnitude (ROM)
 - Information will not be evaluated and is for DARPA planning purposes only



Initial Conceptual Design (ICD)



- Describe key attributes that reflect the government's vision for an operational NCR.
- Provide substantiation that the proposed ICD can meet the evaluation criteria provided in Section 3
 - Initial design does not require rigorous engineering detail and analysis
 - *Proposals should cite the quantitative and qualitative success criteria that the proposed effort will achieve by the time of each Phase's program metric measurement, as well as explain how the proposed effort will achieve those criteria*
- Primary purpose: identify the technology challenges & maturation activities required to enable development of the full-scale NCR
 - It is expected that NCR attributes will evolve throughout the program based on results of individual technology maturation activities and demonstrations
 - This is meant to be an initial look that demonstrates the proposers' understanding of the program objectives, technology challenges, and system integration issues



8.3. Intellectual Property



- **Goal**
 - Develop a cyber testing toolkit suite that the government may provide to any party it authorizes to conduct cyber testing at any authorized facility
- **The Government expects liberal intellectual property rights, including particularly software and technical data, w/ respect to all aspects of the NCR**
- **Liberal intellectual property rights are an expressed element of the Plans and Capability to Accomplish Technology Transition Evaluation Criterion (see Section 7.1.6)**
- **The Government encourages the Contractors to develop software as open source software, insofar as permitted by applicable laws and export regulations**



8.3. Intellectual Property



- **At minimum, the Government requires:**
- **Unlimited Rights to:**
 - Hardware and software interface specification that would enable third-party vendors to develop NCR components and plug-in systems that would seamlessly interface with the performer's range architecture
 - The design of the hardware and software systems that enables the "packaging" and insertion of standard NCR components as peripherals
 - Top-level system specifications, graphics, and performance metrics to enable effective program representation at conferences and trade shows
- **Government Purpose Rights for five (5) years, subsequently reverting to Unlimited Rights, to:**
 - All algorithms, software, protocols, hardware and software interfaces, and accompanying documentation that are not commercial software and are developed or modified under this program
 - Sufficient data to enable independent verification of milestone criteria, test results, performance predictions, and the Contractor's technical and financial progress
 - System details necessary to brief program or component technical progress and accomplishments



8.3. Intellectual Property



- DARPA may choose to accept Limited or Restricted Rights on other items. Additional requirements may later be identified and may become part of future phases. The performer shall be responsible for marking appropriately (by page) all data delivered to the Government to which the Government has less than Unlimited Rights.
- Proposers should not include background proprietary software and data as the basis of their proposed approach unless the proposal includes granting full control to the government. Proposers expecting to utilize, but not to deliver, open source tools or other materials in implementing their approach must ensure that the government does not incur any legal obligation due to such utilization.

Thus, proposals that come with rights other than discussed above will be penalized during the assessment.



Performer Security Requirements



- NCR must test unclassified to Top Secret/Special Compartmentalized Information/Special Access Programs (TS/SCI/SAP).
- Prime team, as well as anyone who would be capable of accessing classified information must have the appropriate clearances and access in accordance with DARPA, DoD and U.S. government policies and procedures.
 - Subcontractors & team members who are developing technologies & procedures, but will not have any access to the tested programs, technologies, data, or test results may not require the same level of clearance.
 - The prime contractor/team leader is responsible to ensure all classified information, programs, technologies, data, & test results are protected in accordance with DARPA, DoD & U.S. government policies & procedures.

Questions: see NCR SCG (DARPA-CG-502) or the DARPA Program Security Representative through the BAA Coordinator.



Funding Restrictions



- **Construction** must be approved in advance and in writing by DARPA.
- All purchases of information technology (IT) must include:
 - Itemized costs or estimated costs
 - Cost justification
 - Letter stating why the proposer cannot provide the requested resources from its own funding
 - Explanation of any estimating factors, including their derivation and application
 - Brief description of the Proposers' procurement method

Awards will not allow reimbursement of pre-award costs



Other



- **Meetings**
 - **Locations**
 - Kickoff - may be conducted in the Washington, D.C. area.
 - All other meetings are expected to be at the performer's location(s)
 - **Purpose**
 - Demonstrate accomplishment and convey information and issues
 - NOT to generate documentation.
 - **Attendance**
 - Tailored based on the agenda: Max 10-20 government

- **Public Release – see Sec 8.7**

- **Conflict of Interest**



Submission Format



- *Proposals not meeting the format described in the BAA may not be reviewed.*
- **Proposers must submit**
 - Original
 - 8 copies of the full proposal
 - 2 electronic copies of the proposal in PDF (preferred) on 2 CD-ROMs
 - Each copy must be clearly labeled with DARPA-BAA-08-43, proposer organization, proposal title (short title recommended), and Copy _ of 8
- *Provide contact information for all sub contractors and teams*

May change to 20 copies



Submittals - Security



- **Volume I (Technical/Management)**
 - May be classified up to SECRET – see page limits { }
- *Volume II (Financial)*
 - *Will be unclassified.*
- *Award document*
 - *Will be unclassified and for follow-on phases may be classified.*
- **You will receive a DD Form 254 “Contract Security Classification Specification” with the classified package**
 - A SECRET facility clearance and a SECRET safeguarding clearance will be required to perform awards issued under this BAA
- **Performers selected to execute Phase II – IV may require additional personnel and facility clearance levels that will be addressed at a later date.**



Proposal Evaluation Criteria



- Ability to Meet Program Go/No-Go Metrics
- Overall Scientific and Technical Merit
- Proposer's Capabilities and/or Related Experience
- Realism of Proposed Schedule
- Potential Contribution and Relevance to the National Cyber Mission
- Plans and Capability to Accomplish Technology Transition
- Cost Realism

Proposals will not be evaluated against each other since they are not submitted in accordance with a common work statement.



Request for Classified Information



- Phase I classified requirements are in the Classified Addendum
 - Classified SECRET
 - Available only to proposer who are cleared to handle such materials

Requests for the Classified Addendum & Security Classification Guide will be accepted only from proposers who complete
Attachment A, DARPA-BAA-08-43 Classified Packet Request Form

- Email the Request Form to BAA08-43@darpa.mil
 - Fax to (703)-807-1762.
 - Subject line: “Request BAA-08-43 Classified Packet”
- Submit this request as soon as possible to allow for adequate time for preparation and delivery.
 - All requestors will receive a confirmation email w/ a tracking number
 - Proof of facility clearance level (FCL) must be validated by the Program Security POC before any classified documentation on the BAA will be sent to the performer



Suspenses



- Suspense for questions May 19
- Q/A published May 23
- Slides published May 23
- Classified Q&A mailed May 27
- Initial Round Proposal Due 4:00 PM Eastern, June 30, 2008

– Original and eight (20) hard and two (2) electronic copies

DARPA/STO (Attn: BAA08-43)
 3701 North Fairfax Drive
 Arlington, VA 22203-1714

Proposals may not be submitted by fax/email - Any sent will be disregarded.

- On contract (C) Fall 2008 ASAP after FY09 Appropriations
- Kickoff C + 30 (Nov 08)
- Phase II-IV Requirements Kickoff + 30 (C + 60)



Agency Contact: BAA Coordinator



- Administrative, technical, contractual questions:
 - unclassified email baa08-43@darpa.mil [fax (703)-807-1762]
 - classified fax (703)-526-4749/50

 - Include
 - Point of contact name, email address, phone number
 - Subject line "BAA 08-43 Question"

- Program Website:
 - <http://www.darpa.mil/sto/solicitations/BAA08-43/index.html>

- Teaming Website:
 - <https://www.davincinetbook.com/teams>

- Program Team
 - Program Manager LTC Michael VanPutte
 - Chief SETA Mr. Larry Blankenship
 - Program Security Rep Mrs. Joanna Chaomalaguti & Mr. Herbert Hinch
 - Programatics Ms. Leanne Wiegand

NOTE: Do not directly contact the contracting officer or program manager with respect to this BAA