



Request for Input (RFI) – National Cyber Leap Year

Overview: This Request for Information (RFI) is issued under the Comprehensive National Cybersecurity Initiative (CNCI), established within Homeland Security Presidential Directive (HSPD) -23. The RFI was developed by the Networking and Information Technology Research and Development (NITRD) Program Senior Steering Group (SSG) for Cybersecurity to invite participation in a National Cyber Leap Year whose goal is an integrated national approach to make cyberspace safe for the American way of life.

Background: We are a cyber nation. The U.S. information infrastructure – including telecommunications and computer networks and systems and the data that reside on them – is critical to virtually every aspect of modern life. This information infrastructure is increasingly vulnerable to exploitation, disruption and destruction by a growing array of adversaries. The President’s CNCI plan calls for *leap-ahead* research and technology to reduce vulnerabilities to asymmetric attack in cyberspace. Unlike many research agenda that aim for steady progress in the advancement of science, the leap-ahead effort seeks just a few revolutionary ideas with the potential to reshape the landscape. These *game-changing* technologies (or non-technical mechanisms that are made possible through technology), developed and deployed over the next decade, will fundamentally change the cyber game into one where the good guys have an advantage. Leap-ahead technologies are so-called because they enable us to leap over the obstacles preventing us from being where we want to be. These advances may require years of concerted research and development to be fully realized, good ideas often do, however the intent is to *start now* and gain momentum as intermediate results emerge.

Objective: The National Cyber Leap Year has two main goals: (1) construction of a national research and technology agenda that both identifies the most promising ideas and describes the strategy that brings those ideas to fruition; and (2) jumpstarting game-changing, multi-disciplinary development efforts.

The Leap Year will run during fiscal year 2009, and will comprise two stages, *prospecting* and *focusing*.

Stage One, which we open with this formal announcement and describe in detail below, canvasses the cybersecurity community for ideas. Our aim is to hear from all those who wish to help.

The heart of Stage Two, which begins February 1, 2009, is a series of workshops to develop the best ideas from Stage One. As the year progresses we will publish four types of findings: (1) *Game-changers*—descriptions of the paradigm-busters that technology will make possible; (2) *Technical Strategy*—as specifically as possible, the invention and/or research which needs to be done; (3) *Productization/Implementation*—how the capability will be packaged, delivered and used, and by whom; and (4) *Recommendations*—prescriptions for success, to include funding, policies, authorities, tasking—whatever would smooth the way to realization of the game-changing capability.

Deadline for Submission under this RFI: We anticipate multiple cycles of Stage One opportunities. The first Stage One cycle is covered by this RFI and will close **December 15, 2008**. Subsequent cycles will be announced by separate RFIs. All Stage One cycles are expected to be complete by April 15, 2009.

Stage One description

What we are looking for:

Contributors may submit up to 3 leap-ahead technology concepts. Multidisciplinary contributions from organizations with cybersecurity interests are especially encouraged. Cognizant of the limits of conventional studies and reports, substantial thought has been given to what framework and methodology might render the community's best ideas understandable, compelling and actionable to those who need to support them, fund them and adopt them. Since our search is for game-changing concepts, we ask that submitters explain their ideas in terms of a game. Many ideas will fall into the following three categories. Ideas that:

Morph the gameboard (change the defensive terrain (permanently or adaptively) to make it harder for the attacker to maneuver and achieve his goals)

Example: non-persistent virtual machines – every time the enemy takes a hill, the hill goes away

Change the rules (lay the foundation for cyber civilization by changing network protocols and norms to favor our society's values)

Example: the no-call list – direct marketers have to “attack” on customer terms now

Raise the stakes (make the cost to play less advantageous to the attacker by raising risk, lowering value, etc.)

Example: charging for email – making the SPAMmer ante up means a lot more fish have to bite for SPAM to pay

Ideas that change the game in some other dimension are also welcome; just be sure to explain how.

Who can participate:

This RFI is open to all and we especially encourage public and private sector groups (e.g. universities, government laboratories, companies, non-profit groups, user groups) with cybersecurity interests to participate. Collaborative, multi-disciplinary efforts are also highly encouraged. Participants in Stage One must be willing to participate in Stage Two should one of their ideas be selected. Participants must also be willing to have their ideas posted for discussion on a public website and/or included in our final report.

How we will use it:

The best ideas from Stage One will go on to Stage Two. Stage One submissions may be posted on our website for elaboration and improvement, as a key goal of the leap year is to engage diverse sectors (e.g. government, academia, commercial, international) in identifying multi-dimensional strategies and, where it makes sense, in rolling up their sleeves and starting to work. Submissions crafted with that larger community in mind will be the most compelling and influential.

Leap Year interim result and emerging guidance will be posted at: www.nitrd.gov/leapyear/.

Questions and submissions should be addressed to: leapyear@nitrd.gov.

In accordance with FAR 15.202(3), responses to this notice are not offers and cannot be accepted by the Government to form a binding contract. Responders are solely responsible for all expenses associated with responding to this RFI, including any subsequent requests for proposals.

All responses must be no more than two pages long (12 pt font, 1" margins) and in this form:

Who you are – name, credentials, group membership

Game-changing dimension – Board, Rules, Stakes?

Concept – What is the idea and why does it change the game?

Vision – Make us believe in your idea (What would the world look like if this were in place? How would people get it, use it? What makes you think this is possible? What needs to happen for this to become real? Which parts already exist; which parts need to be invented?)

Method – What process did you use to formulate and refine your concept? What assumptions or dependencies underlie your analysis?

Dream team – Who are the people you'd need to have on your team to make this real? If you just know disciplines that's OK. If you have names, explain what those people do. If your idea is selected for further consideration, we will do our best to bring these people together for a phase two workshop.

Responses must be submitted via www.nitrd.gov/leapyear/ or emailed to leapyear@nitrd.gov.

Responses to this RFI must be received by December 15, 2008 so that arrangements can be made for Stage Two activities beginning on or about February 1, 2009. Additional Stage One cycles, if any, will be announced by separate RFI with all Stage One activities expected to be complete by April 15, 2009.

Appendix A contains a sample submission and review considerations.

Appendix A

Sample submission

Who you are – quieteveningathome.org – We are a 501c3 group with 50,000 members dedicated to the preservation of the dinner hour as the core of American civilization.

Game-changing dimension – Change the rules

Concept – Telemarketers are using our resources and time to market their products. They can call and interrupt our dinners and use our own telephones to reach us. What if we changed the rules to “don’t call us, we’ll call you?”

Vision – The vision is a national do-not-call register. People should be able to go to donotcall.gov and register their phone number. It would be illegal for telemarketers who have not been given permission to call someone. If a telemarketer makes an illegal call, the recipient should be able to report them to a government agency and they should be fined. The technology to do this is easy, we are not sure about the laws and policies. Courts have ruled differently on this issue at different times. We think the political climate is friendly today for Federal legislation.

Method – we announced our search for ideas on our website and submissions were made there. We also publicized through restaurant and catering associations with whom we often partner, who offered interruption-free free meals for brainstorming sessions. Participation was not limited to members, but could not be anonymous, since it was our intention to follow up with submitters. The Board of Directors of QEAH enlisted the aid of Prandia University to work with the submitters of the best ideas to develop them into even better ideas. The Board ensured all the aspects described in the Leap Year RFI were addressed in our final submissions.

Dream team – Federal Trade Commission, Federal Communications Commission, constitutional lawyer, Telemarketers’ Association, Consumer Union, Oracle or other database company.

Review considerations

Submissions will be reviewed by the NITRD Senior Steering Group for Cybersecurity using the following considerations:

Would it change the game?

How clear is the way forward?

What heights are the hurdles that may be found in the way forward?