

## **Request for Information:**

### **Meshed Wireless Networks**

**Responses Due By: 5:00 PM, U.S. Eastern Standard Time, May 20, 2009**

#### **1. BACKGROUND/PROGRAM DESCRIPTION**

The U.S. Department of Homeland Security (DHS), Science and Technology Directorate (S&T), Explosives Division (EXD), has been tasked to conduct operational field tests of remotely operated and standoff explosive countermeasure technologies to address the threat from suicide bombers, as well as leave-behind and vehicle-borne improvised explosive devices. DHS S&T's Standoff Technology Integration and Demonstration Program (STIDP) is designed to accelerate the development of standoff and remote ly operated explosives detection technologies, related technologies, concepts of operations, and training. The ultimate goal of the program is to prevent explosives attacks at large public events and mass transit facilities via a spiral development approach.

#### **2. PROBLEM STATEMENT/REQUIREMENTS**

The program requires that video from sensor and surveillance cameras is generated, displayed, recorded, archived, and mined over a network for key test parameters. During live operations, video data generated will be displayed and recorded over a network in real time.

The on-site network will deploy wired and/or wireless components to extend reach as well as accommodate different sensors and cameras. However, each site may be different with regard to power availability, area footprint, and location of the command center.

Devices that need to be accommodated include, but are not limited to, next-generation sensors from the infrared, millimeter-wave, radar wave, and terahertz spectrum. We may also be using several different generations of video cameras – high definition, IP-based digital cameras, analog cameras, and smart cameras. The wireless network should be capable of supporting high-bandwidth needs ranging from a few megabits per second to hundreds of megabits per second.

It is imperative that any/all wireless transmissions be secured by open standards-based encryption such as WPA2/AES or better. This includes communications between any cameras/sensors, from cameras/sensors to access points, and between access points.

This RFI is being issued solely for market research, planning and information purposes.

The primary intent of this RFI is to explore innovative wireless technologies. There is a need for a portable, wireless infrastructure on a heterogeneous network comprising smart cameras, high-definition surveillance cameras, and next-generation sensors. This wireless network will need to provide the following capabilities:

1. Must operate indoors and/or outdoors. Must also provide rugged enclosure and mounting accessories to operate in an outdoor environment.
2. Must be able to operate without disruption in areas with high amounts of wireless traffic (e.g. a large, public sporting event: US Tennis Open, NFL Superbowl, Olympic Games, etc.).
3. High bandwidth capacity (greater than 500 megabit/sec) – we are exploring both line-of-site and non-line-of-site, wireless options.
4. Resilience and scalability – either via mesh or via robust, self-reconfiguring setup, using multiple built-in radios, for client and backhaul, per access point.
5. Power – we are seeking technologies that provide **ALL FOUR** of the following power options: Power over Ethernet (PoE 802.3AF), AC, DC, and battery-power as options on a single component. For example, we are not interested in technologies that only are powered by PoE. Each technology product must allow for the use of ALL FOUR of the power options identified above. Non-traditional power options (e.g., solar) could also be considered if justification can be provided for why this is a good solution.
6. Security – supporting current open-source, standards-based encryption of transmitted data (e.g. WPA2, AES).
7. Management software, if applicable, for access point control, firmware upgrade, and configuration.

### **3. RESPONDING TO THIS RFI**

Parties with wireless networking systems that can address the problems and requirements above are encouraged to respond/submit a White Paper. Please limit White Paper submissions to a maximum of 5 pages (including a cover sheet) and provide the following information:

Cover Page (Page 1)

- Contact and company information
  - Name
  - Title

- Company name
- Date of incorporation
- Number of years in business
- FY08 sales
- Number of employees
- Location
- Mailing address
- Phone number
- Website address
- Email address
- Note that RFI respondents shall designate a single point of contact for receipt of all information pursuant to this RFI.
- Name/type of technology or model
- Technology maturity: Existing technology or technology concept
- Technology summary covering technical approach, operating principles, testing conducted to date, and commercial sales, if any

Pages 2-5

- Technical background on how the technology works, and number and type of components.
- Complete list of all standards used to design, fabricate, and test the system, and how those standards were applied to your product (NEMA, ANSI, ASTM, SAE, IEEE, etc.) Be specific. List numbers of standards used and revisions.
- Whether or not the technology is suitable for use outdoors with large crowds.
- Overview of how the technology would be deployed in an operational setting, including hardware, software, and manpower requirements.
- Overview of the test and evaluation conducted to date and how this data supports performance claims.
- Current ongoing R&D and sources of funding (including amounts).
- Schedule for anticipated technology upgrades and associated testing.
- Describe how the technology is or has been or can be integrated with other sensor technologies to improve the overall countermeasure performance.
- Government/academia/industrial partners or potential partners.
- Previous work performed in the subject area being proposed, including but not limited to work performed for the US Government, or other federal agencies (including international).
- Description of how your technology would need to be adapted or integrated with other concealed object detection technologies to provide a viable solution.
- Description of the concealed object detection technologies that could be integrated with your technology to provide a viable solution.

Supporting documentation (such as marketing brochures, fliers, published presentations or papers and other materials that summarize the technology and more about your company) is acceptable (up to 100 pages worth), and may be referenced by reviewers only in support of

claims identified in the White Paper, and only where specifically referenced in the White Paper. The Government makes no guarantee that the supporting documentation will be reviewed and/or considered.

Responses to this request for information are to be submitted electronically to Pacific Northwest National Laboratory (PNNL) at [stidp-rfi@pnl.gov](mailto:stidp-rfi@pnl.gov).

- Please include the RFI number (OPO-09-00000-MWN) in the subject line of your email.
- Method of Submission: One electronic submission in machine-readable format (typically PDF, ASCII, MS Word, or WordPerfect format) should be sent electronically to PNNL.

Submissions must be received no later than 5:00 PM, U.S. Eastern Standard Time, May 20, 2009.

Any company proprietary information, performance capabilities and/or future modification plans should be clearly identified and marked.

Respondents are solely responsible for any and all expenses incurred pursuant to responding to this RFI.

Responses to the RFI will not be returned.

Responses to the RFI may be used to develop Government documentation.

Unsolicited proposals in response to this RFI will not be considered.

#### **4. GOVERNMENT PLANS**

As clearly stipulated in Section 2 of this RFI, the RFI is issued “solely for market research, planning and information purposes” and is not to be construed as a commitment by the Government to issue a subsequent solicitation (Broad Agency Announcement, Request for Proposal, etc.). While the Government, after a detailed review and thorough analysis of the RFI submissions, expects to issue a solicitation that is going to assess the relative maturity of the wireless technologies for detecting threats, it has not committed itself to doing so.

In the event a solicitation is issued, the Government expects that the timing is likely to be in the summer or fall of 2009.

#### **5. CLASSIFIED SUBMISSION**

Classified submissions are not being accepted for the RFI. The eventual solicitation will have provisions to support classified submissions.

Please limit your White Paper responses to this RFI to SSI, company proprietary or unrestricted information, and please mark submissions appropriately. SSI submissions can be submitted as normal by password protecting the document, and then sending the password separately to the contract specialist.

The following is an abbreviated description of SSI:

“SSI is a control designation used by the Department of Homeland Security, and particularly the Transportation Security Administration. It is applied to information about security programs, vulnerability and threat assessments, screening processes, technical specifications of certain screening equipment and objects used to test screening equipment, and equipment used for communicating security information relating to air, land, or maritime transportation. The applicable information is spelled out in greater detail in 49 CFR 1520.7.

When transmitted by e-mail, SSI must be in a password-protected attachment. The password should be transmitted separately of the protected document.”

## **6. REQUESTS FOR ADDITIONAL INFORMATION**

Questions and requests for additional information should be sent to Laboratory (PNNL) at [stidp-rfi@pnl.gov](mailto:stidp-rfi@pnl.gov).