IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER Plaintiff, v. UNITED STATES DEPARTMENT OF HOMELAND SECURITY Defendant.	)	No. 1:11-00945 (ABJ)

PLAINTIFF'S MEMORANDUM OF POINTS AND AUTHORITIES IN OPPOSITION TO DEFENDANT'S MOTION FOR SUMMARY JUDGMENT AND IN SUPPORT OF PLAINTIFF'S CROSS-MOTION FOR SUMMARY JUDGMENT

Plaintiff the Electronic Privacy Information Center ("EPIC") opposes Defendant U.S. Department of Homeland Security's ("DHS") August 22, 2011 Motion for Summary Judgment, and cross-moves for summary judgment in favor of EPIC.

Specifically, EPIC (1) challenges the DHS's withholding of Vaughn Index Documents 5, 8, and 17 and (2) seeks an order compelling the DHS to pay EPIC's fees and costs for this lawsuit, because EPIC qualifies for such relief irrespective of the outcome of the parties' cross-motions for judgment.

FACTUAL BACKGROUND

In 2005, the Transportation Security Administration ("TSA"), a DHS component, began testing Whole Body Imaging ("WBI") technology solely in U.S. airports to examine air travelers on commercial aircraft. WBI devices, which use either backscatter x-ray and millimeter wave technology, capture detailed, three-dimensional images of individuals. The WBI devices literally

peer through clothing to observe and capture an image of the naked human body.

In March 2010, the DHS released a "Surface Transit Security Priority Assessment," which detailed the agency's plans to expand significantly the WBI program and deploy new body scanner technology in America's surface transportation systems, including "mass transit, highways, freight rail, and pipelines…" Body scanner devices had previously been tested at surface transportation stations in both the U.S. and abroad. In 2006, millimeter wave machines were tested on PATH train riders at a New Jersey train station. The DHS has acknowledged that both passive and active millimeter wave technology were employed in this setting. In the summer of 2009, the PATH train system, in conjunction with the Department of Homeland Security, once again tested body scanner technology on PATH travelers.

The DHS has also considered the deployment of mobile WBI technology, referred to as "Z Backscatter Vans." These vans are equipped with concealed WBI devices and are able to scan other vehicles while driving down public roadways and are capable of seeing through vehicles and clothing.

On November 24, 2010, EPIC transmitted, via certified mail, a written FOIA request to the DHS for agency records ("EPIC's FOIA Request"). EPIC requested the following agency records:

> all documents detailing plans by federal law enforcement agencies to implement body scanner technology in the surface transit context;
>
> all contracts, proposals, and communications with private transportation and shipping companies (including, but not limited to NJ PATH, Amtrak, and Greyhound) regarding the implementation of body scanner technology in surface transit;
>
> all contracts, proposals, and communications with states, localities, tribes, and territories (and their subsidiaries or agencies) regarding the implementation of body scanners in surface transportation;
>
> all documents detailing plans by federal law enforcement agencies to use "Z Backscatter Vans" or similar technology;

> all contracts, proposals, and communications with the manufacturers of the "Z Backscatter Vans" or similar technology;
>
> all contracts, proposals, and communications with states, localities, tribes, and territories (and their subsidiaries or agencies) regarding the implementation of "Z Backscatter Vans" or similar technology;
>
> all images generated by the "Z Backscatter Vans" or body scanner technology that has been used in surface transit systems.

The DHS failed to make a timely determination concerning EPIC's FOIA Request, and failed to disclose any records within the FOIA's deadline. The agency did not substantively respond to EPIC until February 16, 2011, two and a half months after EPIC sent its request.

On February 16, 2011, the Science and Technology ("S&T") component of the DHS stated that it had located 1,156 pages of records responsive to EPIC's FOIA request. Of these records, the agency released 15 pages in their entirety, 158 pages in redacted form, and withheld 983 pages in their entirety. On April 14, 2011, EPIC filed an administrative appeal ("EPIC's Appeal") challenging the S&T's withholding of documents. EPIC's Appeal challenged the S&T's partial withholding of 158 pages of documents and the S&T's complete withholding of 983 pages of documents.

The agency failed to comply with the statutory deadline to reply to EPIC's Appeal and EPIC filed suit on May 20, 2011, initiating this lawsuit. On August 15, 2011, following the filing of this suit, the agency disclosed an additional 151 pages in their entirety and 21 pages in redacted form.

As set forth below, EPIC challenges the propriety of the agency's withholdings.

STANDARD OF REVIEW

Summary judgment is appropriate when there is no genuine issue as to the material facts, and the moving party demonstrates it is entitled to judgment as a matter of law. Fed. R. Civ. P. 56; *Diamond v. Atwood*, 43 F.3d 1538, 1540 (D.C. Cir. 1995). FOIA lawsuits are typically resolved on cross-motions for summary judgment. *Reliant Energy Power Generation v. FERC*, 520 F. Supp. 2d 194, 200 (D.D.C. 2007). A court reviews agency handling of a FOIA request *de novo*. 5 U.S.C. § 552(a)(4)(B).

The U.S. Supreme Court "repeatedly has stressed the fundamental principle of public access to Government documents that animates the FOIA." *John Doe Agency v. John Doe Corp.*, 493 U.S. 146, 151-52 (1989). "In enacting FOIA, Congress struck the balance it thought right--generally favoring disclosure, subject only to a handful of specified exemptions--and did so across the length and breadth of the Federal Government." *Milner v. Dep't of the Navy*, 131 S. Ct. 1259, 1266 (2011). As the Court has previously explained, "[t]he basic purpose of FOIA is to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed." *NLRB v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 242 (1978). The FOIA's "basic purpose reflect[s] a general philosophy of full agency disclosure unless information is exempted under clearly delineated statutory language." *Dept. of the Air Force v. Rose*, 425 U.S. 352, 360-61 (1976), quoting S. Rep. No. 813, 89th Cong., 1st Sess., 3 (1965). FOIA was meant to be a "disclosure statute," not a "withholding statute." *Milner*, 131 S. Ct. at 1262.

The FOIA includes exemptions from disclosure, "[b]ut these limited exemptions do not obscure the basic policy that disclosure, not secrecy, is the dominant objective of the Act." *Rose*, 425 U.S. at 361. Therefore FOIA exemptions "must be narrowly construed." *Id*. "The statute's

goal is broad disclosure, and the exemptions must be given a narrow compass." *Milner*, 131 S. Ct. at 1261 (internal citations omitted). Furthermore, "the burden is on the agency to sustain its action." 5 U.S.C. § 552(a)(4)(B); *see also EPIC v. Dept. of Homeland Security*, 384 F. Supp. 2d 100, 106 (D.D.C. 2005).

ARGUMENT

I. FOIA Exemption 5 Does Not Permit the Agency to Withhold Emails, Meeting Minutes, and Briefing Materials

Exemption 5 protects from disclosure "inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency. 5 U.S.C. § 552(b)(5). The exemption is to be applied "as narrowly as consistent with efficient Government operation." *Coastal States Gas Corp. v. Dep't of Energy*, 617 F.2d 854, 868 (D.C. Cir. 1980) *citing* S. Rep. No. 89-813 (1965).

To qualify, a document must satisfy two conditions: "its source must be a Government agency, and it must fall within the ambit of a privilege against discovery under judicial standards that would govern litigation against the agency that holds it." *Dep't of Interior v. Klamath Water Users Protective Ass'n*, 532 U.S. 1, 8 (2001). In order to justify withholding under this exemption, the agency must demonstrate that it meets both requirements; as the United States Supreme Court has pointed out "the first condition of Exemption 5 is no less important than the second; the communication must be 'inter-agency or intra-agency.'" *Id.*

a. *The Documents Are Not "Inter-agency or Intra-agency Memorandums or Letters," and, Thus, Are Not Exempt Under Exemption 5*

As the DHS notes, the Supreme Court has recognized that memorandums prepared by outside experts and consultants can be considered "inter-agency or intra-agency" for the purposes of Exemption 5:

> It is textually possible and . . . in accord with the purpose of the provision, to regard as an intra-agency memorandum one that has been received by an agency, to assist it in the performance of its own functions, from a person acting in a governmentally conferred capacity other than on behalf of another agency-*e.g.,* in a capacity as employee or consultant to the agency, or as employee or officer of another governmental unit (not an agency) that is authorized or required to provide advice to the agency.

U.S. Dept. of Justice v. Julian, 486 U.S. 1, 18 n.1 (1988). However the Court has explained that, in order for materials created or provided by consultants to be exempt under Exemption 5, the consultant must "not represent an interest of its own, or the interest of any other client, when it advises the agency that hires it." *Klamath Water Users*, 532 U.S. at 11. The consultant's "only obligations are to truth and its sense of what good judgment calls for, and in those respects the consultant functions just as an employee would be expected to do." *Id.* Furthermore, when an outside group communicates its views to an agency that are "necessarily adverse to the interests of competitors," the outside group does not act in a consulting capacity. *Citizens for Responsibility & Ethics in Washington v. U.S. Dept. of Homeland Sec.*, 514 F. Supp. 2d 36, 44 (D.D.C. 2007), *citing Klamath Water Users,* 532 U.S. at 15.

In *Klamath Water Users*, the Supreme Court ruled that Native American tribes' communications with the Department of the Interior regarding water rights were not exempt under Exemption 5. The Court held that the tribes were not "consultants" for the purposes of this exemption, because they were communicating with the Bureau "with their own, albeit entirely legitimate, interests in mind," they were "self-advocates at the expense of others seeking benefits inadequate to satisfy everyone." *Klamath Water Users,* 532 U.S. at 12.

The DHS cites several cases to support its proposition that Rapiscan and Northeastern University ought to be considered "consultants" for the purposes of Exemption 5. However, none of the entities in those cases share Rapiscan and Northeastern's self-interest; they acted in "a governmentally conferred capacity." In every case cited by the defendant, the entities in

question were hired to evaluate or perform neutral audits of an already existing agency program. *See Info. Network For Responsible Mining (Inform) v. Dep't of Energy*, CIV. 06-CV-02271-REB, 2008 WL 762248 (D. Colo. Mar. 18, 2008), *Citizens for Responsibility & Ethics in Washington*, 514 F. Supp. 2d 36 (D.D.C. 2007), *Sakamoto v. U.S. Envtl. Prot. Agency*, 443 F. Supp. 2d 1182 (N.D. Cal. 2006), *Citizens Progressive Alliance v. U.S. Bureau of Indian Affairs*, 241 F. Supp. 2d 1342, 1355 (D.N.M. 2002).

In fact, the present case is much more like *Physicians Committee for Responsible Medicine v. National Institutes of Health*, 326 F. Supp. 2d 19, 28 (D.D.C. 2004), in which the D.C. District court ruled that information from a grant applicant, Dr. Podrell, was not exempt under Exemption 5. The court found that the grant applicant's assertion that the application contained patentable, proprietary, and commercial information weighed heavily against his argument that it was an "inter-agency or intra-agency" document. Specifically, the court held that:

> Thus, Dr. Podell's hope of marketing the results of his research cannot be considered an integral part of the agency's deliberative process, but instead must be viewed as an effort taken for his own self-interest. This fact alone distinguishes Dr. Podell's initial grant application from that of a consultant. The distinction is even more evident in that Dr. Podell was in competition with other grant applicants and had a self-interest in being awarded the grant. Thus, even if communications come from paid consultants, which can qualify the communications as intra-agency in nature, they are not entitled to Exemption 5 protection when they come 'from an interested party seeking a Government benefit at the expense of other applicants.'" (internal citations omitted.)

Physicians Comm. for Responsible Med., 326 F. Supp. 2d at 29-30.

Neither Rapiscan nor Northeastern meet the Supreme Court's requirement that a consultant must "not represent an interest of its own, or the interest of any other client, when it advises the agency that hires it." *Julian*, 486 U.S. at 18 n.1.

Northeastern University was engaged in selling its BomDetec program to the Department of Homeland Security. Northeastern has numerous publicly available promotional items

available for the BomDetec program. *See e.g.* Pl. Exhib. 1, 2. These items clearly demonstrate that Northeastern is actively marketing a product. In this case, the synthesis of "four technologies – intelligent video, radar, X-ray, and terahertz – into one surveillance system." Pl. Exhib. 1. The promotional brochure describes the BomDetec product, as well as Northeastern University industry partners (which include Siemens and Raytheon) who are actively working with Northeastern to develop this product.

Rapiscan was also aggressively competing to market body scanners to the Department of Homeland Security. As described in the Defendant's Summary Judgment motion, Rapiscan was awarded a contract to adapt its body scanner devices to standoff detection in mass transit systems. Def.'s Motion for Summ. Judg. at 2-3. Rapiscan and the Defendant have gone to great lengths to describe the adversarial and competitive nature of the body scanner procurement process. *See* Def.'s Motion for Summ. Judg. at 13-16, Modica Dec. ¶ 13. Defendant states "Domestically, there is 'considerable' competition for the provision of scanner systems to the United States, where it is expected that the Transportation Security Administration will procure 500 Advanced Imaging Technology systems in the near term." Modica Dec. ¶ 13. Indeed, even the title of the Rapiscan employee providing the declaration, "Vice President of Product Line Management," Modica Dec. ¶ 1, suggests that this was an exchange between the agency and a "self-advocate[]" who was marketing a product to the agency "at the expense of others seeking benefits inadequate to satisfy everyone." *Klamath Water Users,* 532 U.S. at 12.

At the time that these emails, meeting minutes, and briefing materials were created, both Rapiscan and Northeastern were still engaged in the highly competitive, highly lucrative process of selling a product to the agency. Though they had been granted contracts for development, the biggest prize: the contract for an actual rollout of this technology in rail stations across the

country, had not yet been won. Rapiscan and Northeastern University were communicating with the agency not as independent agents to advance the Department of Homeland Security's interests, but as self-interested actors intent on selling their product to the agency. They were still engaged in an ongoing, intense, high-stakes competition to win large, long-term government contracts. They were communicating with the agency in the same way that the tribes in *Klamath* were: "with their own, albeit entirely legitimate, interests in mind," they were "self-advocates at the expense of others seeking benefits inadequate to satisfy everyone." *Klamath Water Users,* 532 U.S. at 12. Like Dr. Podrell, the grant applicant in *Physicians Committee for Responsible Medicine*, Rapiscan and Northeastern were engaged in a competition with other parties and had self-interest in being awarded further government funds. Hence, the withholding of these three documents under Exemption b(5) was improper, because they are not "inter-agency or intra-agency memorandums or letters." *Id*.

B. The Documents Do Not Qualify for the Deliberative Process Privilege, Because They Contain Factual Information, Not Opinions, Recommendations, or Deliberations

Even if the Court finds that the agency has satisfied the first prong of the Exemption 5 test, the agency has still failed to satisfy the second prong: "it must fall within the ambit of a privilege against discovery under judicial standards that would govern litigation against the agency that holds it." *Klamath Water Users*, 532 U.S. at 8. The agency has withheld emails, meeting minutes, and briefing materials (Vaughn Index Documents #5, 8, and 17), wrongly claiming that they are protected under the deliberative process privilege.

Encompassed in Exemption 5 is the "deliberative process" privilege, which protects from disclosure "documents reflecting advisory opinions, recommendations, and deliberations that are part of a process by which governmental decisions and policies are formulated." *Klamath Water Users,* 532 U.S. at 8.

However, the DHS misstates the definition of "deliberative process" and overstates its scope. In the Vaughn Index, the DHS claims that items #5, 8, and 17 were withheld under the deliberative process privilege because "The release of this internal information would discourage the expression of candid opinions *and inhibit the free and frank exchange of information among agency personnel*." Vaughn Index Items #5, 8, 17 (emphasis added). Setting aside the dispute about whether or not this is actually an exchange of information "among agency personnel," the DHS characterization of Exemption 5 has created a second category of agency records that cannot be properly withheld as deliberative. The purpose of the privilege is to protect "frank discussions of legal or policy matters." *Environmental Protection Agency v. Mink*, 410 U.S. 73, 87, (1972) (finding that the justification for the deliberative process privilege is that "[I]t would be impossible to have any frank discussions of legal or policy matters in writing if all such writings were to be subjected to public scrutiny"); *Dow Jones & Co., Inc. v. Dept. of Justice*, 917 F.2d 571 (D.C. Cir. 1990)(confirming that "[w]e have said that the purpose of Exemption 5 is to encourage the frank discussion of legal and policy issues")(internal citations omitted); *Judicial Watch, Inc. v. U.S. Dept. of Treasury*, 2011 WL 3582152 (D.D.C. Aug. 16, 2011)(finding that the purpose of Exemption 5 is to protect "frank exchange of ideas on legal or policy matters"); S. Rep. No. 89-813 (1965); *see also* H.R. Rep. No. 89-1497 (1966)(stating that "a full and frank exchange of *opinions* would be impossible if all internal communications were made public")(emphasis added). The privilege doesn't exist to protect "the free and frank exchange of *information*," it exists to protect "frank discussions of *legal or policy matters*." *Id.*

Defendant's expansion of this doctrine would include not only discussions of policy, "advisory opinions, recommendations, and deliberations," *Klamath Water Users,* 532 U.S. at 8, but would sweep in all information, even purely factual information, contrary to case law and the

stated purpose of the Exemption. *See Petroleum Info. Corp.*, 976 F.2d at 1434 (D.C. Cir. 1992); S.REP.NO. 89-813 (1965). This is, quite simply, not the purpose or scope of this privilege, as set out by the Supreme Court. *See Klamath Water Users,* 532 U.S. at 8. Neither of the cases cited by the Defendant to support the proposition that the deliberative process privilege protects the "free and frank exchange of *information*" actually support this expansive scope.

Under the deliberative process privilege, factual information generally must be disclosed, but materials embodying officials' opinions are ordinarily exempt. *Petroleum Info. Corp. v. U.S. Dept. of Interior*, 976 F.2d 1429, 1434 (D.C. Cir. 1992), *citing EPA v. Mink,* 410 U.S. at 87-91 (endorsing the fact/opinion distinction); *Quarles v. Department of Navy,* 893 F.2d 390, 392 (D.C.Cir.1990) (observing that "the prospect of disclosure is less likely to make an adviser omit or fudge raw facts, while it is quite likely to have just such an effect" on materials reflecting agency deliberations). "Purely factual reports and scientific studies cannot be cloaked in secrecy by an exemption designed to protect only 'those internal working papers in which opinions are expressed and policies formulated and recommended.'" *Bristol-Myers Company v. FTC,* 424 F.2d 935, 939 (D.C.Cir. 1970) (quoting *Ackerly v. Ley,* 420 F.2d 1336, 1341 (D.C.Cir.1969)).

Specifically, the D.C. Circuit has routinely held that factual information must be released. *Playboy Enterprises, Inc. v. Dep't of Justice*, 677 F.2d 931, 936 (D.C.Cir. 1982) (finding that the factual material in a government report was not protected under the deliberative process privilege and must be released); *Coastal States Gas Corp. v. Dep't of Energy*, 617 F.2d 854, 858 (D.C. Cir. 1980) (holding that memoranda from regional counsel issued in response to requests for interpretations of regulations were not exempt under the deliberative process privilege because they were "straightforward explanations of agency regulations"); *see, e.g., Judicial Watch, Inc. v. U.S. Dept. of Treasury*, CIV.A. 09-01508 BAH, 2011 WL 2678930 (D.D.C. July 11, 2011)

(holding that headers at the top of several sets of minutes were factual and, hence, segregable and must be released),

The Defendant has wrongly withheld purely factual information. The Vaughn Index describes Document #5 as and email from Northeastern representative John Beaty that "outlines and attaches options related to potential test methodology and technology choices to be made, as well as the progression to develop concepts of operation for equipment…" The information contained in this email is largely descriptive and factual. Beaty is not advising the agency, he is not giving opinions, he is simply relaying facts: what the options are, what the process is to develop concepts. Nothing in this Vaughn summary suggests that Beaty is issuing "advisory opinions, recommendations, and deliberations that are part of a process by which governmental decisions and policies are formulated." *Klamath Water Users,* 532 U.S. at 8.

The Defendant has also wrongly withheld purely factual information in Vaughn Index Document #8. This document is meeting minutes describing "options presented to DHS for moving forward with Phase II of system design, a variety of possible deployment scenarios, and the type of software that may need to be developed to effectively manage the system." Def.'s Motion for Summ. Judg. at 21. This document does not detail advisory opinions, recommendations, or deliberations. It simply describes factual details: what options are available, what deployment scenarios exist, and what the parameters are for management software. This document is not within the intended scope of deliberative process privilege.

Similarly, the Defendant's withholding of portions of Vaughn Index Document #17 is improper. This document details the "strengths and weaknesses of the prototype system," which is exactly the type of factual information that courts typically find is not protected by the deliberative process privilege.

C. Even if the Court Finds that Portions of the Documents Are Protected Under the Deliberative Process Privilege, the Unprotected Factual Portions Are Segregable and Should Be Released

Even if the agency establishes that it has properly withheld portions of these documents under FOIA Exemption 5, "it must nonetheless disclose all reasonably segregable, nonexempt portions of the requested record(s)." *Roth v. U.S. Dep't of Justice,* 642 F.3d 1161, 1167 (D.C.Cir. 2011); *North v. U.S. Dep't of Justice,* 774 F.Supp.2d 217, 222 (D.D.C.2011) (citing *Oglesby v. U.S. Dep't of the Army,* 79 F.3d 1172, 1178 (D.C.Cir. 1996)). The agency bears the burden of demonstrating that withheld documents contain no reasonably segregable factual information. *Mokhiber v. U.S. Dept. of Treasury*, 335 F. Supp. 2d 65, 69 (D.D.C. 2004), *citing Army Times Pub. Co. v. Department of Air Force,* 998 F.2d 1067, 1068 (D.C.Cir. 1993); *Mead Data Central, Inc. v. U.S. Dept. of Air Force,* 566 F.2d 242, 260 (D.C.Cir. 1977). Here, the DHS has not clearly demonstrated in the Vaughn Index that the documents contain no reasonably segregable factual information.

Even if the Court finds that Rapiscan and Northeastern were consultants for the purposes of the "inter-agency or inter-agency" requirement, and even if the Court finds that portions of these records contain "advisory opinions, recommendations, and deliberations that are part of a process by which governmental decisions and policies are formulated," *Klamath Water Users,,* 532 U.S. at 8, all segregable factual portions of the records must still be released. *See Roth v. U.S. Dep't of Justice,* 642 F.3d at 1167. As discussed above, the Vaughn Index presented by the Defendant contains many references to information that is most likely factual. Thus, even if the Court finds that there is a section of Vaughn Index Document #17, for example, that contains an advisory opinion regarding what the agency should do about the weaknesses of the prototype

system, the agency must still disclose the underlying factual information: what the strengths and weaknesses were.

II. FOIA Exemption 4 Does Not Permit the Agency to Withhold Emails, Meeting Minutes, Briefing Materials, and Other Records

The DHS alleges that the emails, meeting minutes, and briefing materials discussed above are also exemption from disclosure under Exemption 4. The agency has also wrongly withheld additional information under Exemption 4, which protects "trade secrets and commercial or financial information obtained from a person and privileged or confidential." 5 U.S.C. § 552(b)(4). In order to qualify for this exemption, the information must meet all three requirements. The agency's withholdings in this case do not meet the third requirement: the information must be "privileged or confidential." *Id.*

A. The Withheld Information is Not Subject to Exemption 4 Because it is Already Publicly Available

In *National Parks and Conservation Ass'n v. Kleppe*, 498 F.2d 765 (D.C. Cir. 1974), the court found that the test for commercial information is an objective one requiring a showing of likely specific harm. Commercial or financial information is confidential "if disclosure of the information is likely to have either of the following effects: (1) to impair the government's ability to obtain the necessary information in the future or (2) to cause substantial harm to the competitive position of the person from whom the information was obtained." *Id.* at 770.

Courts have found that "[p]ublic availability of information defeats an argument that the disclosure of the information would likely cause competitive harm." *Nat'l Cmty. Reinvestment Coal. v. Nat'l Credit Union Admin.*, 290 F. Supp. 2d 124, 134 (D.D.C. 2003). "To the extent that any data requested under FOIA are in the public domain, the submitter is unable to make any claim to confidentiality-a *sine qua non* of Exemption 4." *CNA Fin. Corp. v. Donovan*, 830 F.2d

1132, 1154 (D.C. Cir. 1987); *see also Worthington Compressors, Inc. v. Costle,* 662 F.2d 45, 51 (D.C. Cir. 1981) (finding that "[i]f the information is freely or cheaply available from other sources, such as reverse engineering, it can hardly be called confidential and agency disclosure is unlikely to cause competitive harm to the submitter"); *Critical Mass Energy Project v. Nuclear Regulatory Comm'n*, 975 F.2d 871, 872 (D.C. Cir. 1992) (holding that information "will be treated as confidential under Exemption 4 if it is of a kind that the provider would not customarily make available to the public").

Despite its insistence that the public release of this information would harm its ability to compete, Rapiscan, itself, has already disclosed much of this information in widely available brochures, product information data sheets, and websites. This public availability negates the argument that disclosure would harm Rapiscan or impair the government's ability to obtain necessary information in the future. *Nat'l Cmty. Reinvestment Coal.,* F. Supp. 2d at 134.

The Vaughn Index doesn't specifically identify which particular security device is at issue here, but the Modica Declaration and Defendant's Motion for Summary Judgment indicate that it is the Secure 1000 and possibly the Wave 200. The Secure 1000 is the commonly used airport body scanner machine, which uses backscatter x-rays. The Wave 200 is a passive millimeter wave machine, designed for use in "high throughput inspection." Pl. Exhib. 6.

1. Secure 1000: Publicly Available Information

As Plaintiff's Exhibits 3-5 demonstrate, Rapiscan has already publicly released many of the same details regarding the Secure 1000 that it is now attempting to claim are confidential. Plaintiff's Exhibit 3 is a promotional data sheet by Rapiscan for its Secure 1000 scanner. This brochure is publicly available on Rapiscan's website[1] and contains several classes of information

[1] http://www.rapiscansystems.com/en/products/item/productsrapiscan_secure_1000_dual_pose

that the agency has identified as "confidential" in the Vaughn Index and Motion for Summary Judgment: scan time (Vaughn Index Items #6-10, 12), inspection time (Vaughn Index Items #6-10, 12), design schematics (Vaughn Index Item #9, 10), detection abilities (Def.'s Motion for Summ. Judg. at 15), and images of how the system would identify threats (Vaughn Index Item #9).

Plaintiff's Exhibit 4 is a document available on the New York Office of General Services Website.[2] This document lists in detail the 2009 pricing for a variety of Rapiscan Products, including the "Secure 1000 (5000 Series) - Windows, standard resolution," and a variety of accessories for the system including the backdrop, operator table, and privacy algorithms. Similar information is also available elsewhere, including mainstream media sources, such as Bloomberg Businessweek. Pl. Exhib. 5. This is precisely the "unit pricing" information that the defendants are attempting to argue is confidential. Vaughn Index Item #8, 15; Def.'s Motion for Summ. Judg. at 15.

2. Wave 200: Publicly Available Information

Plaintiff's Exhibits 6-7 demonstrate that many of the details regarding the Wave 200 have also already been publicly released. Plaintiff's Exhibit 6 is a promotional data sheet produced by Rapiscan. This data sheet contains several classes of information that the agency has identified as "confidential" in the Vaughn Index and Motion for Summary Judgment: frequency requirements (Vaughn Index Items #6-10), scan time (Vaughn Index Items #6-10), design schematics (Vaughn Index Item #9, 10), detection abilities (Def.'s Motion for Summ. Judg. at 15), and images of how the system would identify threats (Vaughn Index Item #9, 10).

[2] *www.ogs.state.ny.us/purchase/spg/pdfdocs/3823219745PL_Rapiscan.pdf*

Plaintiff's Exhibit 7 is an item from Bloomberg Businessweek, detailing unit pricing for the Wave 200. This is, again, the "unit pricing" information that the defendants are attempting to argue is confidential. Vaughn Index Item #8, 15; Def.'s Motion for Summ. Judg. at 15.

EPIC does not dispute certain agency withholdings, including employee information and specific cost breakdowns. But EPIC does dispute the withholding of the agency records described *supra*. The public availability of this information precludes the assertion of Exemption 4. *Nat'l Cmty.*, 290 F. Supp. 2d at 134.

B. Segregable Portions Must Be Released

As discussed above, if a document contains exempt information, the agency must still release "any reasonably segregable portion" after deletion of the nondisclosable portions. 5 U.S.C. § 552(b); *Oglesby v. U.S. Dept. of Army*, 79 F.3d 1172, 1176 (D.C. Cir. 1996). The agency has withheld five records in full and four in part under Exemption b(4). The statute requires that any portions of these records that are not properly exempt must be released.

III. EPIC Is Entitled to Recover Its Costs and Fees

A. EPIC "Substantially Prevailed" by Forcing Disclosure of DHS Records

Irrespective of the outcome of the parties' cross-motions for summary judgment, EPIC is entitled to recover its fees and costs from the DHS in this matter. EPIC asks the Court to enter judgment as to EPIC's eligibility and entitlement to fees and to order further briefing as to the amount of costs and fees. "The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this section in which the complainant has substantially prevailed." 5 U.S.C. § 552(a)(4)(E). "A complainant has substantially prevailed if the complainant has obtained relief through … a voluntary or unilateral change in position by the agency, if the complainant's claim is not insubstantial." *Id*. The

determination of whether the plaintiff has "substantially prevailed" is "largely a question of causation." *Weisberg v. Dep't of Justice*, 745 F.2d 1476, 1496 (D.C. Cir. 1984); *Church of Scientology v. Harris*, 653 F.2d 584, 587 (D.C. Cir. 1981). The key inquiry is "did the institution and prosecution of the litigation cause the agency to release the documents obtained during the pendency of the litigation?" *Church of Scientology*, 653 F.2d at 587.

EPIC has already "substantially prevailed" in this lawsuit. As described above, EPIC filed its FOIA request concerning body scanners on November 24, 2010. On April 16, 2011, EPIC filed an administrative appeal challenging the DHS's wrongful withholding of documents. On May 20, 2011, EPIC filed this lawsuit challenging the agency's wrongful withholding of documents. On August 15, 2011, the agency disclosed an additional 151 pages of documents in their entirety and 21 pages in redacted form. "The institution and prosecution" of this suit plainly "cause[d] the agency to release the documents obtained during the pendency of the litigation."

B. The Court Should Award EPIC Costs and Fees In This Case

"The court should consider [four factors] in determining the appropriateness of an award of costs and attorney fees." *Cuneo v. Rumsfeld*, 553 F.2d 1360, 1365 (D.C. Cir. 1977). The four factors are: 1) "the benefit to the public, if any, deriving from the case;" 2) "the commercial benefit of the complainant;" 3) "the nature of [the complainant's] interest in the records sought"; and 4) "whether the government's withholding of the records sought had a reasonable basis in law." H. Comm. on Gov't Operations and S. Comm. on the Judiciary, 94th Cong., *Freedom of Information Act and Amendments of 1974 (Pub. L. No. 93-502) Source Book,* 189-90 (J. Comm. Print 1975).

"Public benefit" can be demonstrated by a "newsman . . . seeking information to be used in a publication or a public interest group . . . seeking information to further a project benefiting

the general public." *Id*. at 171. The "public benefit" factor supports an award where the complainant's victory is "likely to add to the fund of information that citizens may use in making in making vital political choices." *Cotton v. Heyman*, 63 F.3d 1115, 1120 (D.C. Cir. 1995) (citations omitted). D.C. District court has found that news media coverage is relevant for determining "public benefit." *Elec. Privacy Info. Ctr. v. U.S. Dept. of Homeland Sec.,* 2011 WL 4014308 (D.D.C. Sept. 12, 2011).

EPIC's FOIA suit provided substantial benefit to the public. EPIC maintains two of the most popular websites in the world - www.epic.org and www.privacy.org - for searches on the term "privacy." EPIC disseminated the agency records it received on its www.epic.org web site[3] and to the approximately 8,000 recipients of its bi-weekly newsletter.[4] EPIC's FOIA work in this matter was prominently featured in a Forbes article:

> Giving Transportation Security Administration agents a peek under your clothes may soon be a practice that goes well beyond airport checkpoints. Newly uncovered documents show that as early as 2006, the Department of Homeland Security has been planning pilot programs to deploy mobile scanning units that can be set up at public events and in train stations, along with mobile x-ray vans capable of scanning pedestrians on city streets.

Andy Greenberg, "Documents Reveal TSA Research Proposal To Body-Scan Pedestrians," Train Passengers, Forbes, Mar. 2, 2011.[5] Other news organizations reported on the agency's development of mobile body scanners *See, e.g.,*. Thomas Frank, *Homeland Security Looked Into Covert Body Scans*, USAToday, Mar. 3, 2011;[6] Jaikumar Vijayan, *DHS Seeks Systems for Covert*

[3] http://epic.org/2011/08/documents-reveal-new-details-a.html
[4] http://epic.org/alert/epic_alert_1818.html
[5] http://www.forbes.com/sites/andygreenberg/2011/03/02/docs-reveal-tsa-plan-to-body-scan-pedestrians-train-passengers/
[6] http://www.usatoday.com/news/washington/2011-03-04-bodyscans04_ST_N.htm

Body Scans, Documents Show, ComputerWorld, Mar. 3, 2011.[7] Members of Congress have also demonstrated interest in the topic of mobile body scanners. Joe Pyrah, *Chaffetz: Mobile Scanners Invade Privacy*, The Daily Herald, Aug. 29, 2010.

"Commercial benefit to the complainant" might preclude an award if the beneficiary is a "large corporate interest (or a representative of such an interest)." *Freedom of Information Act and Amendments of 1974 Source Book* at 171. However, commercial benefit does not bar recovery "where the complainant was indigent or a nonprofit public interest group." *Id.* In fact, nonprofit organizations are "the sort of requester that Congress intended to recover attorney's fees under FOIA." *Elec. Frontier Found. v. Office of the Director of National Intelligence*, 2008 WL 2331959 (N.D. Cal. June 4, 2008). EPIC is a 501(c)(3) non-profit public interest research center. EPIC derived no commercial benefit from its FOIA request or lawsuit. The sole benefit was derived by the public, which benefited from the disclosure of the body scanner documents released in this case.

The "nature of the [complainant's] interest" factor is "closely related [to] and often considered together" with the commercial benefit criterion. *Tax Analysts v. Dep't of Justice*, 965 F.2d 1092, 1095 (D.C. Cir. 1992) Favored interests are "scholarly, journalistic or public-interest oriented." *Freedom of Information Act and Amendments of 1974 Source Book* at 171. *See Long v. IRS*, 932 F.2d 1309, 1316 (9th Cir. 1991) (holding that a lower court's ruling that the plaintiff's scholarly interest weighed against her recovery of fees was held "wrong as a matter of law and an abuse of discretion."). As set forth above, EPIC's interest in this matter is squarely within the "scholarly, journalistic or public-interest oriented" interests favored by the statute.

---

7 http://www.computerworld.com/s/article/9212681/DHS_seeks_systems_for_covert_body_scans_documents_show

See, e.g., Elec. Privacy Info. Ctr. v. United States Dep't of Homeland Sec., 760 F. Supp. 2d 4, 44 (D.D.C. 2011) ("[EPIC's] aims, which include dissemination of information regarding privacy issues to the public, . . . fall within the scholarly and public-interest oriented goals promoted by FOIA, . . .")

The DHS did not have a "reasonable legal basis" for failing to disclose records to EPIC. The DHS's delay in replying to EPIC's request and appeal plainly violated the FOIA's statutory deadlines. *See* 5 U.S.C. § 552(a)(6)(A). As described in EPIC's Complaint, the DHS violated statutory deadlines by failing to make a timely determination concerning EPIC's administrative request and appeal. Compl. at ¶¶28-32. The DHS has cited no legal basis in opposition to EPIC's claims regarding the untimeliness of the agency's response. An agency's representation that records were not produced more quickly due to processing backlogs, confusion, and administrative error are "practical explanations, not reasonable legal bases" for withholding. *Miller v. Dep't of State*, 779 F.2d 1378, 1390 (8th Cir. 1985). "The FOIA does not contain a statutory exception for administrative inefficiency. When a private citizen is obliged to seek legal services in order to wrest from the government information which the government had no legal reason to withhold from him, he is entitled under the Act to be reimbursed for the cost to which he has been put." *Id.* Nor did DHS cite any legal basis for withholding the 172 pages of documents that it later disclosed on August 15, 2011.

In this case, EPIC was forced to sue the DHS in order to wrest from the government critical information concerning the DHS' mobile body scanner program. The DHS had no reason or legal basis to withhold these records. The agency must reimburse EPIC for its costs and fees.

CONCLUSION

As discussed above, Defendant's Motion for Summary Judgment should be denied as to the withholdings under Exemption 5 and all segregable portions of documents withheld under Exemption 4. In addition, Plaintiff is entitled to recover its costs and fees because it has "substantially prevailed" in this case regardless of the outcome of the parties' cross-motions for summary judgment. A proposed Order is attached.

Respectfully submitted,

/s/ John Verdi

JOHN VERDI (DC Bar # 495764)
MARC ROTENBERG (DC Bar # 422825)
GINGER MCCALL (DC Bar # 1001104)
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
Counsel for Plaintiff

Dated: September 22, 2011

CERTIFICATE OF SERVICE

I hereby certify that on the 22nd day of September 2011, I served the foregoing PLAINTIFF'S MEMORANDUM OF POINTS AND AUTHORITIES IN OPPOSITION TO DEFENDANT'S MOTION FOR SUMMARY JUDGMENT AND IN SUPPORT OF PLAINTIFF'S CROSS-MOTION FOR SUMMARY JUDGMENT, including all exhibits and attachments, by electronic case filing upon:

JAVIER M. GUZMAN
Assistant United States Attorney
U.S. Department of Justice

/s/ John Verdi
John Verdi
Counsel for Plaintiff

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER Plaintiff, v. UNITED STATES DEPARTMENT OF HOMELAND SECURITY Defendant.	)	No. 1:11-00945 (ABJ)

PLAINTIFF'S STATEMENT OF MATERIAL FACTS
NOT IN GENUINE DISPUTE

In accordance with LCvR 7(h), Plaintiff the Electronic Privacy Information Center submits this statement of material facts not in genuine dispute in support of its cross motion for summary judgment.

1. On November 24, 2010, EPIC transmitted, via certified mail, a written FOIA request to the DHS for agency records ("EPIC's FOIA Request"). EPIC requested the following agency records:

   a. all documents detailing plans by federal law enforcement agencies to implement body scanner technology in the surface transit context;

   b. all contracts, proposals, and communications with private transportation and shipping companies (including, but not limited to NJ PATH, Amtrak, and Greyhound) regarding the implementation of body scanner technology in surface transit;

   c. all contracts, proposals, and communications with states, localities, tribes, and territories (and their subsidiaries or agencies) regarding the implementation of body scanners in surface transportation;

   d. all documents detailing plans by federal law enforcement agencies to use "Z Backscatter Vans" or similar technology;

e. all contracts, proposals, and communications with the manufacturers of the "Z Backscatter Vans" or similar technology;

f. all contracts, proposals, and communications with states, localities, tribes, and territories (and their subsidiaries or agencies) regarding the implementation of "Z Backscatter Vans" or similar technology;

g. all images generated by the "Z Backscatter Vans" or body scanner technology that has been used in surface transit systems.

Compl., ¶ 16; Medina Decl., ¶ 8, Def. Motion for Summ. Judg.

2. The DHS failed to make a timely determination concerning EPIC's FOIA Request, and failed to disclose any records within the FOIA's deadline. *Medina Decl.* at ¶24.

3. The agency first disclosed documents on February 16, 2011. *Medina Decl.* at ¶24.

4. EPIC appealed the redactions within these documents. Compl., ¶ 28-31.

5. The DHS failed to make a timely response to EPIC's administrative appeal. Compl., ¶ 32.

6. EPIC filed suit concerning EPIC's First FOIA Request on May 20, 2011, initiating this lawsuit. *Complaint*, Dkt. No. 1., *EPIC v. DHS*, No. 11-00945 (D.D.C. filed May 20, 2011).

7. Subsequent to this action being filed, the DHS made a second document disclosure on August 15, 2011. *Medina Decl.* at ¶25.

8. The agency has since completed its search for, and production of, records responsive to EPIC's FOIA Requests. *Medina Decl.* at ¶25.

9. The DHS has withheld nine records under Exemption 4 – five in full and four in part. Def.'s Motion for Summ. Judg. at 12; *Medina Decl.* at ¶19.

10. The DHS has withheld three records under Exemption 5 – two in full and one in part. Def.'s Motion for Summ. Judg. at 18; *Medina Decl.* at ¶22.

Respectfully submitted,

/s/ John Verdi

JOHN VERDI (DC Bar # 495764)
MARC ROTENBERG (DC Bar # 422825)
GINGER MCCALL (DC Bar # 1001104)
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
Counsel for Plaintiff

Dated: September 22, 2011

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER Plaintiff, v. UNITED STATES DEPARTMENT OF HOMELAND SECURITY Defendant.	)	No. 1:11-00945 (ABJ)

PLAINTIFF'S STATEMENT OF GENUINE ISSUES IN OPPOSITION TO DEFENDANT'S STATEMENT OF MATERIAL FACTS

In accordance with LCvR 7(h), Plaintiff the Electronic Privacy Information Center submits this statement of genuine issues in opposition to Defendant's statement of material facts.

14. **Defendant's alleged fact:** "In an effort to narrow the issues for judicial review, DHS, subsequent to the filing of this action, has further reviewed the records to determine whether any additional non-exempt information could be reasonably segregated."

Genuine issue: Defendant cites Ms. Medina's declaration to support this statement, but Ms. Medina's declaration says nothing to support the proposition that the agency reviewed records "in an effort to narrow the issues for judicial review." EPIC disputes this characterization. Insofar as the agency contends that it reviewed and released documents in response to EPIC's lawsuit, EPIC has no factual dispute.

Respectfully submitted,

/s/ John Verdi

JOHN VERDI (DC Bar # 495764)
MARC ROTENBERG (DC Bar # 422825)
GINGER MCCALL (DC Bar # 1001104)
Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
Counsel for Plaintiff

Dated: September 22, 2011

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER Plaintiff, v. UNITED STATES DEPARTMENT OF HOMELAND SECURITY, Defendant.	)	No. 1:11-00945 (ABJ)

[PROPOSED] ORDER

Upon consideration of Defendant's Motion for Summary Judgment, Plaintiff's Opposition and Cross-motion for Summary Judgment, and any opposition and replies thereto, it is hereby

ORDERED that Defendant's Motion is DENIED, and it is further

ORDERED that Plaintiff's Motion is GRANTED, and it is further

ORDERED that Defendant disclose to Plaintiff, within seven (7) days of the date of this order, all documents withheld under Exemption 5 and all segregable portions of documents withheld under Exemption 4, and it is further

ORDERED that Plaintiff is eligible for, and entitled to, recover its reasonable costs and attorneys fees incurred in this matter, and it is further

ORDERED that Plaintiff shall file a Bill of Costs and Fees with the Court within thirty (30) days of the date of this order.

So ordered on this _____ day of _____, 2011

_____
AMY BERMAN JACKSON
United States District Judge

EXHIBIT 1

October 01, 2006

BomDetec - wide area surveillance and suicide bomber detection

John Beaty
Northeastern University

Richard Sullivan
Northeastern University

Carey M. Rappaport
Northeastern University

BomDetec – Wide Area Surveillance and Suicide Bomber Detection

John Beaty, Richard Sullivan, Carey M. Rappaport
Department of Electrical Engineering, Northeastern University, MA 02115

This work was supported in part by CenSSIS, the Center for Subsurface Sensing and Imaging Systems, under the Engineering Research Centers Program of the National Science Foundation (Award Number EEC-9986821)

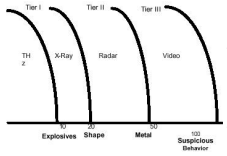
Abstract

Amidst the manifold threats currently afflicting society, that of body-worn explosives is significant if not altogether paramount. Veiled under layers of clothing by individual suicide bombers, these explosives are often constructed of non-standard parts, making detection at a safe distance difficult. It behooves us to develop a detection system capable of locating such explosives at distances sufficient to prevent suicide bombers from approaching densely populated or strategically important areas. Funded by the Department of Homeland Security, the intent of this project is to synthesize four technologies—intelligent video, radar, X-ray, and terahertz—into one surveillance system for suicide bomber detection. Ideally, bombers will be identified at distances of up to fifty meters. Using intelligent video, bombers will be identified visually, prompting the operation of the other three technologies all aimed in the direction of the identified suspect. These three additional sensors will, together, detect and confirm the presence of metal and explosive materials on the person. Radar will be capable of detecting the presence of metal at distances equal to or greater than 50m. At closer distances—>10m—x-ray backscatter will be capable of confirming metal and detecting explosives. At still closer distances—~10m—Terahertz (THz) radiation will sense and spectroscopically identify the explosives. The synthesis of these four technologies, with the signal processing and graphic interfaces necessary to make them useful, hinges on the cooperation of the industry partners: Northeastern University (NEU), AS&E, PPT, Raytheon, Rensselaer Polytechnic Institute (RPI), and Siemens.

Problem Description

- Explosive devices, most often consisting of cylindrical, metal objects filled with explosives, require detection by radar, x-ray backscatter, and terahertz technology.
- Testing protocols must be developed to model realistic conditions.
- Unique scattering patterns may be obtained using a cross-polarized signal, but existing radar can only facilitate one polarization.
- Existing radar aperture does not result in desired beam width.

Four Technologies



General Overview

Suicide bombers are a relevant and tangible threat to human lives on a daily basis. Armed with body-worn explosives, bombers enter buildings or outdoor, densely populated crowds and detonate improvised explosive devises (IEDs) worn on their person. The majority of an IED's construction consists of explosives packed in metal objects. The metal objects are necessary to the bomber's aims, acting as shrapnel upon detonation. To avoid visible detection, these metal objects take on a shape and construction agreeable to being worn about the human torso as shown in Figure 1. A cylindrical or pipe-bomb shape is common.

While their typical construction is the cause of an IED's danger, it also renders it susceptible to detection. A variety of technologies are capable of detecting either the bomb's metal construction or its explosive material. When synthesized into a single, cohesive system, these technologies provide an effective means to identify and apprehend suicide bombers before they can remit their destructive deeds.

Figure 1 – Reproduction of typical body-worn explosive

The BomDetec project intends to synthesize four specific technologies – intelligent video, millimeter wave (MMW) radar, x-ray backscatter, and terahertz spectroscopy – into a single detection system for suicide bombers. The schematic for the proposed system is shown in Figure 2. The applications for this system are varied; from embassies, to train stations, to military facilities, any building or location commonly targeted by suicide bombers.

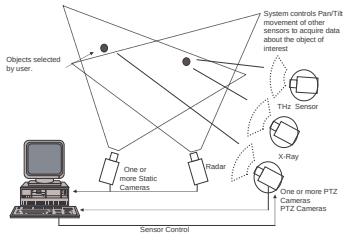


Figure 2 – Schematic of BomDetec System

Intelligent Video

Industry Partners: SIEMENS

The first tier of security in the integrated system is intelligent video. The purpose of intelligent video is to enable the system operator (security agent or someone of like responsibility) to locate suspicious behavior or appearance visually at distances exceeding 50m and to isolate individuals for further detection.

Siemens has previously developed technologies capable of facilitating intelligent video in varying crowd densities and environmental conditions. The technology is capable of distinguishing humans from background objects and other clutter and tracking individuals as they move. Sample results of this system are shown in Figure 3. The right-most image of Figure 3 illustrates how the intelligent video outputs may be transferred to a plan view.

Figure 3 – Siemens' Intelligent Video Technology

In order to facilitate integration with the complete BomDetec system, Siemens envisions a number of improvements to the multiple, stationary cameras with pan, tilt, zoom (PTZ) intelligent video in order to account for the case when an object is occluded or visible by only one camera.

The intelligent video system will use an object's 3D predicted location in order to aim the other three sensors. Siemens is experienced in providing the geometric calibration modules necessary for each of the three sensors to interface with the intelligent video. Once a subject has been visually identified with the BomDetec system, the MMW radar, x-ray backscatter, and terahertz spectroscopy technologies will be focused to that individual.

MMW Radar

Industry Partners: Northeastern University, Raytheon, PPT

Millimeter wave (MMW) radar is effective at detecting metal objects. Metal objects are very effective at scattering electromagnetic waves. These scattered waves are detected by the radar and, using imaging techniques, processed into an practical visual quantification of the level and shape of metal present .

Since we desire our radar to operate at a distance of up to 50m, we wish for the 3dB beam width to subtend an arc that corresponds roughly to the width of an average human torso. If we take the desired distance to be 50m and the width of a human torso to be approximately 0.5m, we find that 0.01 rad or 0.57° is the desired 3dB beam width.

Existing Radar

For initial testing in the MMW radar portion of the BomDetec project, Raytheon is providing a rectangular aperture antenna. With this antenna, the radar industry partners intend on testing a variety of subjects under a variety of conditions in order to determine the radar's capability to identify metallic objects typical of IEDs.

As previously mentioned, we desire a narrow beam width in order to illuminate one human body with an antenna beam as illustrated in Figure 4. A rectangular aperture's 3dB beam width as:

$$\Theta_{3dB} = 50.6\lambda / a \ \ (\text{deg})$$

Where a is the horizontal dimension of the rectangular aperture. Raytheon's antenna is approximately 12cm in its horizontal dimension and operates at 77GHz, giving a 3dB beam width of 1.64°. Given that we require a beam width of 0.57°, we also require a rectangular aperture with a horizontal dimension of about 34cm, three times the size of aperture we have for testing. One possible solution for the testing phase is to focus the existing antenna on a offset scanning confocal paraboloid in order to increase the aperture image and decrease the beam width.

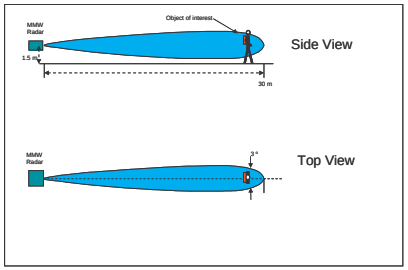


Figure 4 – Radar Illuminating a Human Body

PPT has already performed preliminary testing with a different radar system, attempting to record scattered fields from a variety of objects: human bodies with or without metal cylinders and with or without attached nails. PPT found that metal objects worn on the body by means of attachment to a vest do produce a significant backscatter signal as shown in Figure 5.

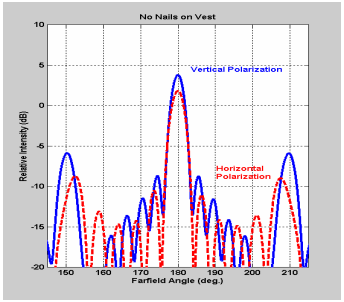


Figure 5 – Radiation Intensity Plot of Bomb Vest

X-Ray Backscatter

Industry Partners: AS&E

At closer distances, say 10 to 20m, the BomDetec system will activate an X-Ray Backscatter system in order to further confirm the presence of metal objects worn by a suspect. X-Ray Backscatter provides more resolution than does the radar system and can provide information, such as location on body and shape, about the explosives. A sample of the sort of images attainable with this technology is shown in Figure 6.

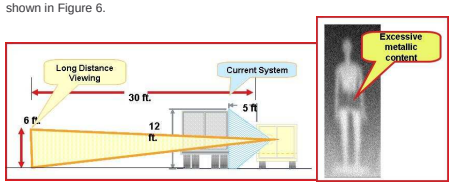


Figure 6 – (Left) A Schematic of AS&E's current X-Ray Van System. (Right) X-Ray Backscatter Image of a "Suicide Bomber" at 30ft (10 meters) from Interrogation Source.

Terahertz Radiation

Industry Partners: Rensselaer

Terahertz (THz) radiation technology will be used to examine suspects at the closest distances – ~10m – in order to confirm the presence of explosive materials. THz technology exploits the absorption spectra that are specific to certain molecules in order to identify dangerous materials, since many molecules show sharp absorption features in the THz range. Figure 7 shows an example of these peaks along with the specific spectroscopic characteristics of certain explosive materials in Table 1.

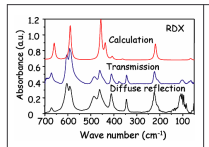


Figure 7 – An example of THz signature in explosive material (RDX).

	Measured resonance (cm^{-1}) "THz signatures"
TNT	123,157,180,319,325,355,463,703,639
Tetryl	109,237,276,489,518,612
RDX	100,225,345,410,461,488,589,605
HMX	83,202,370,399,452,484,606,617
2-mmo-1,6-DNT	28,46,122,169,209,283,329,259,495,488,556
4-mmo-2,6-DNT	41,47,152,168,194,251,310,340,371,462,499,566
4-Nitrotoluene	81,257,295,361,468,522,617
1,2,3-TNB	129,174,235,375,460,525,635
1,3-DNB	78,163,352,406,511,571
1,4-DNB	108,132,155,346,415,443,507,518
2,4-DNT	68,84,107,296,352,396,427,478,527,635
2,6-DNT	52,82,99,187,225,320,381,444,463,510,575

Table 1, THz signatures in explosive materials. Newly found peaks at RPI are shown in red.

It is thought that even the enclosures of explosives may themselves lend a unique absorption spectra. However, given the erratic and uncommon nature behind materials used in improvised explosives, this is not likely an area of the technology that will be pursued.

Future of BomDetec

Currently in Phase I, BomDetec industry partners are working with their existing sensors, testing them in suicide bomber situations in order to determine their potential contribution to the overall project. If a sensor proves reliable and suitable for the breadboard arrangement sought in Phase II, it will be included. Otherwise, sensors and other systems may require additional design prior to Phase II.

As it is the intention of this project to mount the system within a van, it will be the responsibility of AS&E to integrate all sensors into their Z Backscatter Van. Furthermore, it will be the responsibility of Siemens to generate the software necessary for sensor integration, including all the data handling algorithms and systems. Siemens will also be responsible for designing the graphic user interface (GUI) (and the for the BomDetec System.

Upon completion of Phase I, Northeastern University, with its industry partners, will produce a final report that will constitute a preliminary design report.

References

1) Center for Subsurface Sensing and Imaging Systems (CenSSIS), " BomDetec – Wide Area Surveillance and Suicide Bomber Detection at >10M: Volume I – Core Technical Proposal,", September 16, 2005.

EXHIBIT 2

Northeastern University

ALERT Awareness and Localization of Explosives-Related Threats

A Department of Homeland Security Center of Excellence

INDUSTRIAL COLLABORATION

ALERT takes advantage of existing relevant research strengths of The Bernard M. Gordon Center for Subsurface Sensing and Imaging Systems (Gordon-CenSSIS). Gordon-CenSSIS is an existing NSF-funded Engineering Research Center, with a mission to develop new technologies to detect hidden objects and to use those technologies to meet real-world societal challenges in areas as diverse as noninvasive breast cancer detection or underground pollution assessment.

The ERC is supported by and collaborates actively with 20 affiliate organizations representing sectors such as: Medical Imaging (Analogic, Siemens, Hologic, Massachusetts General Hospital), Defense and Intelligence (American Science & Engineering, Raytheon, National Geospatial Intelligence Agency, Lockheed Martin, Textron Systems, INL and LLNL), Civil and Environmental Sensing (TransTech, Boston Groundwater Trust, Woods Hole Oceanographic Institution, Geophysical Survey Systems), and Advanced Computation and Data Handling. In its seven-year history, Gordon-CenSSIS has produced 289 refereed papers, 426 conference publications and graduated 88 PhD and 31 MS students.

Gordon-CenSSIS has an outstanding track record for creating effective university-industry teams oriented to address important DHS problems. One example is the Advanced Spectroscopic High Energy Radiation Detector (ASHERD) Program to detect threatening nuclear material in truck and shipboard containers. An NU-led team in combination with Bubble Technologies Inc. (BTI), a Gordon-CenSSIS industrial partner, researched and created a prototype model, which enabled Raytheon (another Gordon-CenSSIS industrial partner) to win an ~$400 million Advanced Spectroscopic Portal (ASP) production contract from DHS. Another example is the multi-sensor suicide bomber detection program, (BomDetec), currently being funded in Phase I by DHS. This effort includes two ALERT partner universities (NU, RPI) and four industry partners (AS&E, Raytheon, Siemens, and PSI) in a proof-of-concept program to demonstrate the effectiveness of combining multi-sensor probes with a human-in-the-loop video tracking system. Other pending university-industry proposals include a passive IR explosive detection system and a proposal in preparation to create a pervasive layered reconnaissance capacity for ports of entry. This seamless teaming with industry is a hallmark of the ALERT program.

EXHIBIT 3

Rapiscan Secure 1000®

Rapiscan® systems
An OSI Systems Company

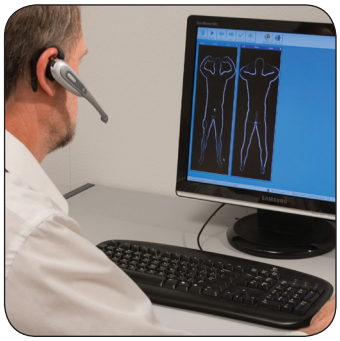
PEOPLE SCREENING

Hands-Off Screening

Quick and Effective

Privacy Protection

High Resolution Imaging



Shown with Communications Monitor Option

The **Rapiscan Secure 1000**® is the most effective people screening solution available. The system produces high resolution images that enable the operator to easily identify concealed threat and contraband items. The Rapiscan Secure 1000 is ideal for high security environments because both organic (e.g. solid and liquid explosives, narcotics, ceramic weapons) and inorganic (e.g. metal) materials are apparent in the image.

Rapiscan Systems has developed advanced techniques to protect the privacy of the person being screened while enabling effective detection of threat items. In a recent study, 95% of persons preferred a Secure 1000 scan to an invasive pat down physical search. The system is deemed safe for all persons and exceeds the requirements of health authorities worldwide.

The Rapiscan Secure 1000 incorporates design improvements that resulted from a deployment of the system at London Heathrow Airport. The Secure 1000 is the first backscatter personnel screening solution to be deployed in the civil aviation environment.

The dependable Rapiscan Secure 1000 is easy to use and is the most widely deployed image-based people screening solution.

The Rapiscan Secure 1000 features:

Rapiscan Systems' Patented **Low Z Backdrop option** extends detection coverage of subjects and speeds throughput. Competitive systems from other vendors require additional scan positions to achieve comparable levels of detection performance; thereby lowering throughput and increasing operating costs. The Rapiscan Secure 1000 **Low Z Backdrop option** is recommended for high throughput and high security screening environments.

The **communications monitor option** (patent pending) enables a remotely located image inspector to provide status indications and search instructions to the local machine operator.

Applications

AVIATION SECURITY

MILITARY BASE SECURITY

CORRECTIONAL FACILITIES

BORDER CROSSINGS

Customer Support

Our team is dedicated to providing a prompt, effective and personalized response that exceeds your expectations. With spare parts inventory and skilled technicians all over the world, you can be certain Rapiscan Systems will always be prepared with a solution to address your requirements. By measuring response time, parts delivery and support status, our team embraces a customer focused philosophy to ensure continual improvement in customer support, products and services.

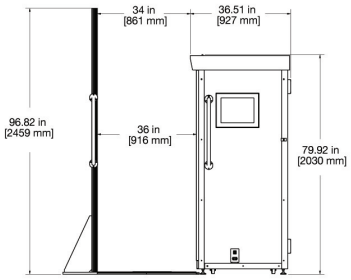
Rapiscan® systems

An OSI Systems Company

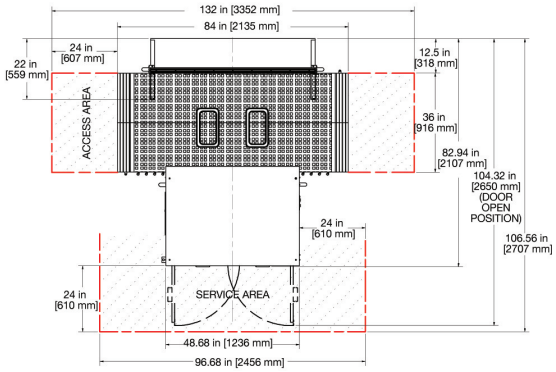
Rapiscan Secure 1000®

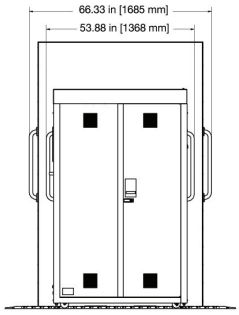
PEOPLE SCREENING

PHYSICAL DIMENSIONS
(Units in inches and mm)

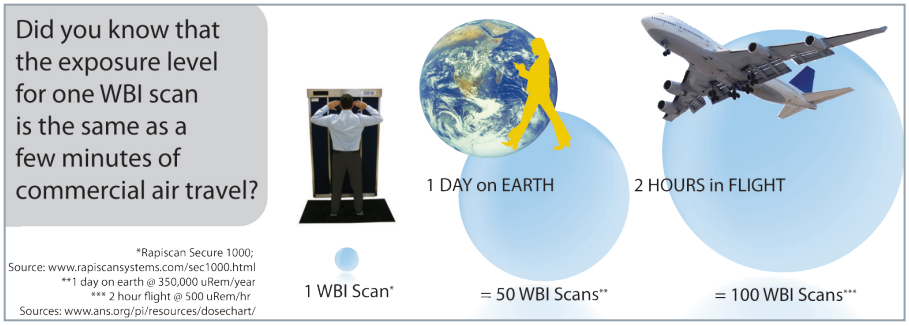


Shown with optional back panel and optional communications monitor





SPECIFICATIONS	
Regulatory Compliance & Safety	The Rapiscan Secure 1000® complies with the applicable FDA requirements and ANSI Standards. The FDA has classified the Rapiscan Secure 1000 as a device under Section 201(h) of the Federal Food Drug and Cosmetic Act (FFDCA) and the safety of the product is addressed by the provisions of Subchapter C – Electronic Product Radiation Control. The Rapiscan Secure 1000 has been assigned the FDA Succession number 9110663-03. The ANSI Standard is N43.17 and is titled "Radiation Safety for Personnel Screening Systems Using X-ray".
Compliance	CE UL
Image Acquisition	Scan rate: Less than 7 seconds per view Display: 19 inch high-resolution color monitor Emission Per Scan: Less than 10 microRem
Power Specifications	115V systems: 115V single phase, 60Hz, 12 Amps 230V Systems: 220-240V single phase, 50/60Hz, 6 Amps
Operating Environment	Storage Temperature: 0°C to 50°C Operating Temperature: 0°C to 40°C Relative Humidity: 5 to 95% non-condensing
Physical Details (excludes optional backpanel)	Floor Space: 6.6 ft. wide x 8.8 ft. length (2001 x 2691 mm) in front Overhead Clearance: 80 in. (204 cm) minimum Unit Weight: 1097 pounds (499 kilograms) Physical Dimensions: 48.7 in. wide x 36.5 in. deep x 80 in. high (1236 x 927 x 2030 mm)
Warranty	One year



X-RAY COMPARISONS: Some of the typical exposure levels that can be experienced with other types of X-ray systems and some naturally occurring sources.

ISO 9001:2000 Certified

CERTIFICATION: The United States Department of Homeland Security has certified the Rapiscan Secure 1000 as an approved product for homeland security. For more information please visit www.safetyact.gov.

With continual development of our products Rapiscan Systems reserves the right to amend specifications without notice.

9150068-9

www.rapiscansystems.com • sales@rapiscansystems.com

AMERICAS, CARIBBEAN
2805 Columbia Street
Torrance, California 90503
UNITED STATES of AMERICA
Tel: +1 310-978-1457
Fax: +1 310-349-2491

EUROPE, MIDDLE EAST, AFRICA
X-Ray House
Bonehurst Road
Salfords
Surrey RH1 5GG
UNITED KINGDOM
Tel: +44 (0) 870-7774301
Fax: +44 (0) 870-7774302

ASIA
240 Macpherson Road
#07-03 Pines Industrial Building
Singapore 348574
SINGAPORE
Tel: +65-6743-9913
Fax: +65-6743-9915

AUSTRALIA
Rapiscan House
4 Ross Street
South Melbourne Victoria
Australia 3205
AUSTRALIA
Tel: +61 3 9929 4600
Fax: +61 3 9929 4655

distributor stamp

051109

EXHIBIT 4

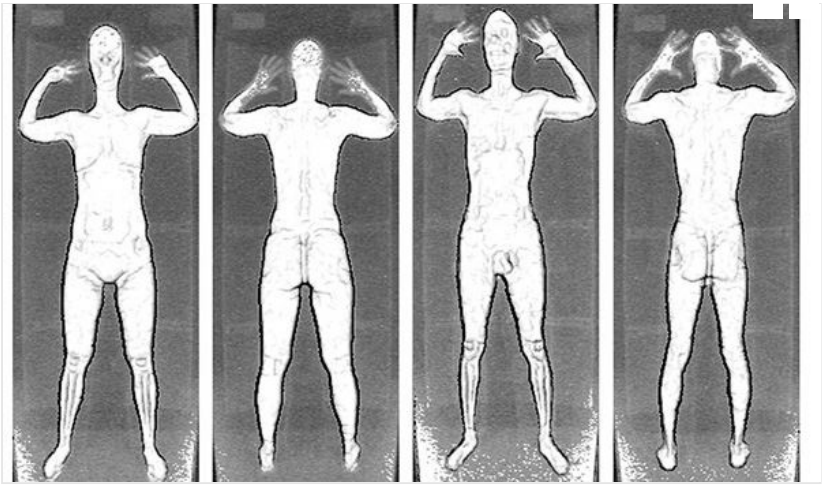
Rapiscan 12-09 Price List

Item#	ItemDesc	Mfr	MfrItem#	Category	Unit of Measure	CatPrice	Discount%	NetPrice
600 Series - Baggage and Parcel Inspection								
1	RAP 618XR--115V	Rapiscan	618XR-W115	38232	1	$23,295.00	17.385%	$19,245.16
2	RAP 618XR--230V	Rapiscan	618XR-W230	38232	1	$23,295.00	17.385%	$19,245.16
3	RAP 620XR--115V	Rapiscan	620XR-W115	38232	1	$33,120.00	17.385%	$27,362.09
4	RAP 620XR--230V	Rapiscan	620XR-W230	38232	1	$33,120.00	17.385%	$27,362.09
5	RAP 622XR--115V	Rapiscan	622XR-W115	38232	1	$37,260.00	17.385%	$30,782.35
6	RAP 622XR--230V	Rapiscan	622XR-W230	38232	1	$37,260.00	17.385%	$30,782.35
7	RAP 624 115/230	Rapiscan	624XR	38232	1	$40,365.00	17.385%	$33,347.54
8	RAP 626 115/230	Rapiscan	626XR	38232	1	$40,365.00	17.385%	$33,347.54
9	RAP 627XR--115V	Rapiscan	627XR-W115	38232	1	$43,470.00	17.385%	$35,912.74
10	RAP 627XR--230V	Rapiscan	627XR-W230	38232	1	$43,470.00	17.385%	$35,912.74
11	RAP 632	Rapiscan	632XR	38232	1	$82,800.00	17.385%	$68,405.22
Secure 1000 - People Screening								
12	Secure 1000 (5000 Series) - Windows, standard resolution, all customers	Rapiscan	2034534	38232	1	$119,025.00	11.340%	$105,527.57
13	220V conversion - Option only at time of order	Rapiscan	2334539	38232	1	**N/C**		
14	Backdrop - For enhanced detection for all models	Rapiscan	2334538	38232	1	$9,315.00	11.340%	$8,258.68
15	Operator Table	Rapiscan	2344531	38232	1	$3,105.00	11.340%	$2,752.89
16	Network option - 5000 and 6000 series only	Rapiscan	2313658	38232	1	$5,175.00	11.340%	$4,588.16
17	Privacy algorithm (non TSA) - 5000 and 6000 series only (Enhanced Imaging Option)	Rapiscan	SW930184	38232	1	$10,350.00	11.340%	$9,176.31
18	UPS	Rapiscan	5610567	38232	1	$3,105.00	11.340%	$2,752.89
19	UPS	Rapiscan	5610577	38232	1	$3,105.00	11.340%	$2,752.89
20	Training Simulator Option	Rapiscan	2334528	38232	1	$6,727.50	11.340%	$5,964.60
21	Training Image Library Option	Rapiscan	SW930203	38232	1	$5,175.00	11.340%	$4,588.16
22	Crystal Clear	Rapiscan	SecureCC	38232	1	$10,350.00	11.340%	$9,176.31
23	Locking Console Option	Rapiscan	SecureLC	38232	1	$3,726.00	11.340%	$3,303.47
24	Second Computer Option	Rapiscan	Secure comp2	38232	1	$2,587.50	11.340%	$2,294.08
25	Scanner Monitor	Rapiscan	Secure scanmon	38232	1	$3,105.00	11.340%	$2,752.89
Metal Detectors								
26	Metor 300 Multi-Zone Walk Through Metal Detector	Rapiscan	8100718	38232	1	$7,762.50	23.430%	$5,943.75
27	Metor 200 HS High Sensitivity Multi-Zone Walk Through Metal Detector	Rapiscan	8100300	38232	1	$7,245.00	35.520%	$4,671.58

Rapiscan 12-09 Price List

Item#	ItemDesc	Mfr	MfrItem#	Category	Unit of Measure	CatPrice	Discount%	NetPrice
28	Metor 200 HDe Enhanced High Discrimination Multi-Zone Walk Through Metal Detector	Rapiscan	8100595	38232	1	$7,245.00	23.430%	$5,547.50
29	Metor 200 Multi-Zone Walk Through Metal Detector	Rapiscan	3885349	38232	1	$6,210.00	31.9938%	$4,223.19
30	Metor 28 Hand Held Metal Detector	Rapiscan	8100374	38232	1	$207.00	49.625%	$104.28

EXHIBIT 5



Rapiscan Systems' Rapiscan Secure 1000
Another Rapiscan body screener, the Secure 1000 uses an ultralow-dose X-ray to produce high-resolution images that let security personnel identify weapons and liquid explosives. Built-in software conceals the identity of the person being screened. Officials at airports, jails, and military checkpoints have deployed more than 200 Secure 1000 and prior-generation machines worldwide. The system costs $130,000.

EXHIBIT 6

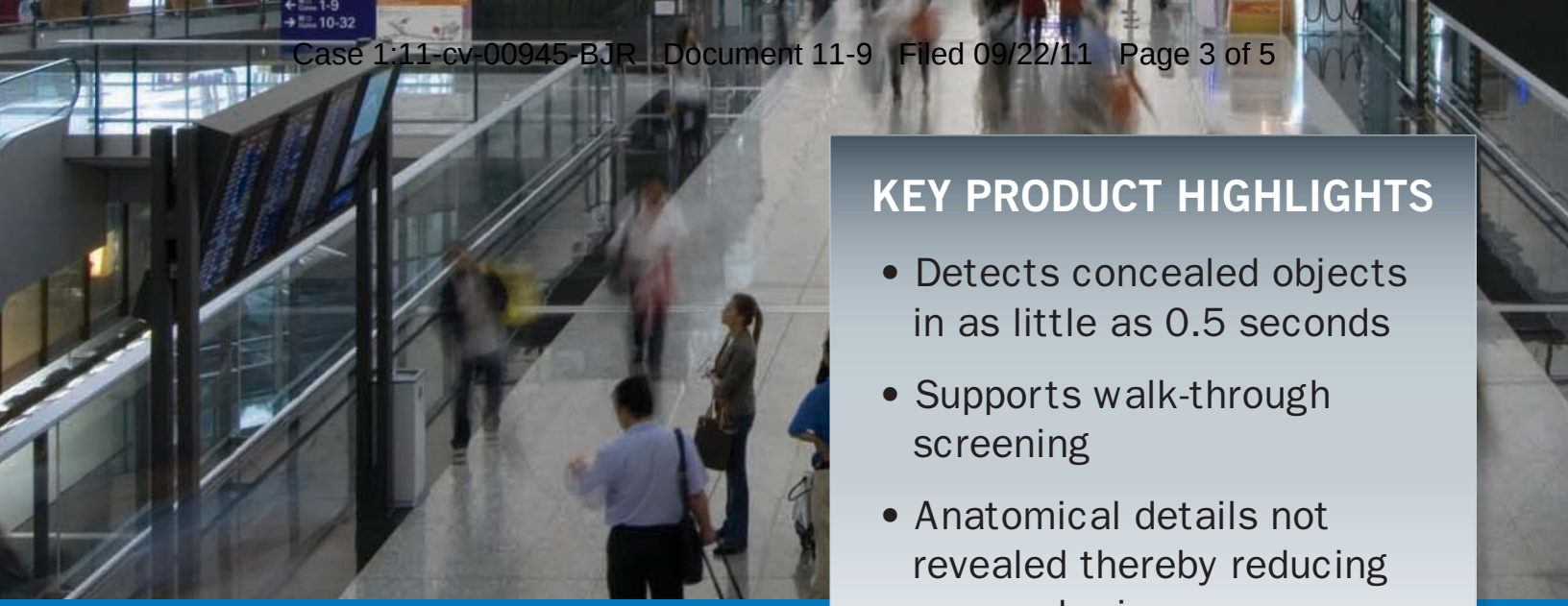
Introducing the

Rapiscan WaveScan 200

Passive Millimeter Wave People Screening System

Rapiscan® systems
An OSI Systems Company

ONE COMPANY - TOTAL SECURITY



Rapiscan WaveScan 200

The Rapiscan WaveScan 200 uses passive millimeter wave technology to provide additional levels of flexibility and capability to address challenging personnel screening and object detection requirements. Designed for high throughput inspection, military, Homeland Security and commercial applications, the WaveScan 200 can be used as a stand-off solution or combined with Rapiscan Systems' other screening and detection products to provide a fully integrated checkpoint system.

KEY PRODUCT HIGHLIGHTS

- Detects concealed objects in as little as 0.5 seconds
- Supports walk-through screening
- Anatomical details not revealed thereby reducing personal privacy concerns
- Passive system — no transmission of radiation
- Integrates with remote operation and legacy checkpoint systems
- Provides standoff detection of large explosives, liquids and gels

GRAPHICAL USER INTERFACE

Rapiscan Systems' **Graphical User Interface (GUI)** is an easy to understand tool - operators can identify hidden objects without confusion or delay. With training, a WaveScan 200 user can identify and locate hidden objects in realtime by observing event icons and detection boxes on a fullmotion video images. Each event's video and passive millimeter wave images are digitally archived for later review, analysis, or evidentiary use. The JPEG images stored are millimeter wave images with no anatomical detail, thereby addressing privacy concerns.

The Rapiscan WaveScan 200: A Proven Technology

The Rapiscan WaveScan 200's passive millimeter wave technology has been proven in government and commercial applications worldwide. The WaveScan 200 gives customers new capabilities and greater return on their existing security investments.

Perimeter Security: For military, Homeland Security and critical infrastructure protection, the Rapiscan WaveScan 200's stand-off and remote operation capabilities allow customers to identify persons approaching a security perimeter with concealed objects – before threats reach the perimeter or security personnel.

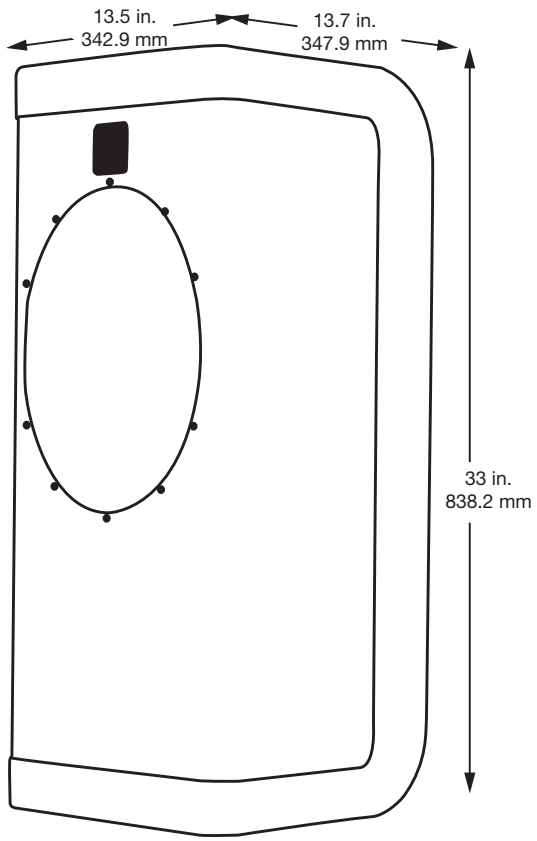
Integrated Checkpoint: For aviation, military, transportation, courthouse, embassy and other security requirements, the Rapiscan WaveScan 200's ability to rapidly detect a wide range of concealed objects can make checkpoints more effective. Used at the beginning of a checkpoint process, the WaveScan 200 can quickly identify persons who have not divested themselves of concealed objects so that they can be isolated and given additional screening.

Customs and Border Control: For customs and border security, the Rapiscan WaveScan 200 allows enforcement personnel to determine whether persons are carrying concealed objects before they leave the control and declaration area.

Pilfering, Theft and Smuggling Prevention: The Rapiscan WaveScan 200 can be used to rapidly screen persons as they exit or enter a warehouse, corrections institution, or classified document environment to determine if they are concealing objects ranging from paper to electronics to narcotics.

SPECIFICATIONS	
Power Supply	External Supply, 100 to 240 VAC, 47-63 Hz, 120 W; output 12 VDC, 10 A
Detector Millimeter Wave Frequency	80 to 100 GHz (90 GHz center frequency, 20 GHz bandwidth)
Operating Temperature	-10°C to 50°C (14°F to 122°F)
Operating Humidity	0 to 100% RH condensing (outdoor use)
Dimensions (H X W X D):	83.8 cm x 34.5 cm x 34.9 cm (33.0 in x 13.5 in x 13.7 in) excluding mounting bracket
Weight	Net: approx. 39 kg (86 lbs) - excluding mounting bracket

INTERFACES	
Analog video output	NTSC or PAL, BNC connector
Monitor output	D-sub 15 (VGA) connector (1024 x 768 72 Hz default)
Control, setup and monitoring	10/100 Ethernet, RJ45
Peripheral interface	Two USB 2.0; two IEEE 1394a (FireWire)
Keyboard/Mouse	Combined PS/2-type mini-DIN connector
Discrete I/O	10 Position Phoenix™ connector; three user-defined outputs (dry contact Form C relay) and two user-defined inputs (opto-isolated)
Audio	One 3.5 mm jack for LINE OUT; one 3.5 mm jack for MIC IN



Rapiscan® systems
An OSI Systems Company

USA - CALIFORNIA
2805 Columbia Street
Torrance, California 90503
UNITED STATES of AMERICA
Tel: +1 310-978-1457
Fax: +1 310-349-2491

USA - WASHINGTON DC
1530 Wilson Blvd, Ste 170
Arlington, VA 22209-2413
UNITED STATES of AMERICA
Tel: +1 703-812-0322
Fax: +1 703-812-0335

UNITED KINGDOM
X-Ray House
Bonehurst Road
Salfords
Surrey RH1 5GG
UNITED KINGDOM
Tel: +44 (0) 870-7774301
Fax: +44 (0) 870-7774302

SINGAPORE
240 Macpherson Road
#06-04 Pines Industrial Bldg
Singapore 348574
SINGAPORE
Tel: +65-6743-9892
Fax: +65-6743-9885

ASIA PACIFIC
Rapiscan House
4 Ross Street
South Melbourne Victoria
Australia 3205
AUSTRALIA
Tel: +61 3 9929 4601
Fax: +61 3 9929 4655

E-MAIL
sales@rapiscansystems.com

WEB
www.rapiscansystems.com

EXHIBIT 7

Rapiscan Systems' Rapiscan WaveScan 200

Designed for screening people, the WaveScan 200 uses a full-motion video camera and so-called millimeter wave technology, which beams radiation over a body's surface, to detect potentially harmful objects carried close to the body. To protect privacy, the WaveScan 200 doesn't capture images of anatomical details. Available since 2004, the system costs $100,000 and is used by customs agents around the world.