NPS-LM-06-013

ACQUISITION RESEARCH WORKING PAPER SERIES

Cookies for the Real World: Assessing the Potential of RFID for Contractor Monitoring

30 May 2006

by

Dr. Nicholas Dew, Assistant Professor
Naval Postgraduate School

Prepared for: Naval Postgraduate School, Monterey, California 93943

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL

The research presented in this report was supported by the Acquisition Chair of the Graduate School of Business & Public Policy at the Naval Postgraduate School.

To request Defense Acquisition Research or to become a research sponsor, please contact:

NPS Acquisition Research Program
Attn: James B. Greene, RADM, USN, (Ret)
Acquisition Chair
Graduate School of Business and Public Policy
Naval Postgraduate School
555 Dyer Road, Room 332
Monterey, CA 93943-5103
Tel: (831) 656-2092
Fax: (831) 656-2253
e-mail: jbgreene@nps.edu

Copies of the Acquisition Sponsored Research Reports may be printed from our website www.nps.navy.mil/gsbpp/acqn/publications

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL

About the Working Paper Series

This article is one in a series of papers addressing one or more issues of critical importance to the acquisition profession. A working paper is a forum to accomplish a variety of objectives, such as: (1) present a rough draft of a particular piece of acquisition research, (2) structure a "white paper" to present opinion or reasoning, (3) put down one's thoughts in a "think piece" for collegial review, (4) present a preliminary draft of an eventual article in an acquisition periodical, (5) provide a tutorial (such as a technical note) to accompany a case study, and (6) develop a dialogue among practitioners and researchers that encourages debate and discussion on topics of mutual importance. A working paper is generally the "internal" outlet for academic and research institutions to cultivate an idea, argument or hypothesis, particularly when in its infant stages. The primary intent is to induce critical thinking about crucial acquisition issues/problems that will become part of the acquisition professional body of knowledge.

It is expected that articles in the working paper series will eventually be published in other venues, such as in refereed journals and other periodicals, as technical reports, as chapters in a book, as cases or case studies, as monographs, or as a variety of other similar publications.

Readers are encouraged to provide both written and oral feedback to working- paper authors. Through rigorous discussion and discourse, it is anticipated that underlying assumptions, concepts, conventional wisdom, theories and principles will be challenged, examined and articulated.

THIS PAGE INTENTIONALLY LEFT BLANK

Abstract

The purpose of this paper is to draw together in one place knowledge that is relevant to the possible role of RFID (radio frequency identification) in contractor monitoring. The paper uses multiple case studies and internet survey methods to explore several issues in RFID-enabled monitoring of contractors. It also offers some conceptual frameworks to help decision makers think through ways RFID might emerge as a contractor monitoring technology as well as some of the key reasons for using this mechanism of monitoring. The paper concludes with research challenges and key issues for practitioners.

THIS PAGE INTENTIONALLY LEFT BLANK

About the Author

Nick Dew is an assistant professor in the Graduate School of Business and Public Policy at the Naval Postgraduate School, Monterey, CA. Nick has a Ph.D. in management from the University of Virginia, and an MBA from the Darden Business School, as well as a BA in history from the University of York in the U.K. Before joining academia, Nick worked in strategic management and sales & marketing for British Petroleum, Europe's largest company, including a two year assignment in BP headquarters and a three-year international assignment in Southeast Asia.

Nick joined the faculty at the Naval Postgraduate School in 2003 where he teaches strategic management in the MBA program. He researches the evolution of the RFID (radio frequency identification) industry and entrepreneurial decision making. His work has appeared in the *Journal of Evolutionary Economics*, the *Journal of Business Venturing,* the *International Journal of Entrepreneurship and Innovation* and the *Scandanavian Journal of Management*. For more information on entrepreneurial decision making, go to www.effectuation.org.

Nick Dew
Assistant Professor
Graduate School of Business and Public Policy
Naval Postgraduate School
Monterey, CA 93943-5197
Tel: (831) 656-3622
E-mail: ndew@nps.edu

THIS PAGE INTENTIONALLY LEFT BLANK

NPS-LM-06-013

ACQUISITION RESEARCH WORKING PAPER SERIES

Cookies for the Real World: Assessing the Potential of RFID for Contractor Monitoring

30 May 2006

by

Dr. Nicholas Dew, Assistant Professor
Naval Postgraduate School

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

Introduction **1**

SECTION I: SOME BASIC INTUITIONS ABOUT THE OPPORTUNITIES FOR APPLYING RFID TO THE PROBLEMS IN CONTRACTOR MONITORING **5**

Understanding RFID as a disruptive technology 5

RFID possibilities as a monitoring technology 9

SECTION II: RFID AS A MONITORING TECHNOLOGY: CASE EXAMPLES **15**

Where did the idea of directly tagging people come from? 15

Case studies of RFID applied to human subjects monitoring 16

Synthesizing the case studies 24

SECTION III: WILL THEY WEAR IT? – PRIVACY ISSUES **27**

The survey 28

CONCLUSION **33**

List of References **35**

Initial Distribution List **37**

THIS PAGE INTENTIONALLY LEFT BLANK

Introduction

The purpose of this paper is to draw together in one place knowledge that is relevant to the possible role of RFID (radio frequency identification) in contractor monitoring, i.e. to attempt to pull together what we know about this issue at the current point in time. The scope of the paper is limited to non-combat military contracting. The content of the paper is mainly empirical: I will use multiple case studies and internet survey methods to explore what I see as the important issues in monitoring contractors, some of which turn out to be quite general. For example, it is impossible to use RFID for collecting information on contractors without also invading the privacy of individuals that are tagged. Because individuals' rights to privacy are defended constitutionally, normatively and by the actions of special interest groups, I explore privacy issues in the paper at some length. After all, RFID tagging will only generate information if contractors wear the tags; and even then some information may be illegal to use or its use might be eliminated by contract provisions.

Monitoring issues are endemic in any contractual relationship. Take a routine service such as hiring a nanny to watch small children while parents are at work. How will we know the service has been performed properly and to our specifications? How can we monitor it in order to tell? How will we know if we have been over-billed? Traditionally parents might have relied on a variety of mechanisms to "police" their nanny, such as spot checks, job screening and social reputation. But in recent years parents have begun to apply new technology to the nanny monitoring problem too, by installing "nanny cams" that enable them to watch home from work, via the internet. The example – deliberately chosen because it is mundane – highlights two issues in monitoring. First, monitoring is costly because it requires a monitor; and second, new technologies are emerging that make it possible to monitor more efficiently.

Of course, the costs of monitoring contractors are hardly new. In ancient Egypt the Pharoah Khasekem faced the problem of how to monitor food distribution

among 100,000 men working on pyramid construction. He had to hire a battery of administrators just to account for food rations, so that some workers could not successfully take more than their daily food allowance. This meant developing the ability to individually identify workers, and account for food rations given to them. Then, as now, the costs of monitoring were apparent in the cost of administrative personnel and systems that were necessary in order to monitor worker behavior (Ezzamel, 2004).

The use of technologies in monitoring is not a new insight either: weighing and measuring technologies have always influenced how goods are sold, a well-known example being de Beers method of batching rough diamonds and selling them on a take-it-or-leave-it basis (Foss and Foss, 2005). Technology availability governs what kinds of contracts are possible by affecting what kinds of monitoring is possible, and therefore how work might be optimally organized. Among new technologies, video is one way of monitoring, but there are others. Software cookies monitor internet surfers' by tracking their "clicks" as they browse the web, and in the process generate information about an individual's movement around the internet. RFID (radio frequency identification) tags worn by individuals generate "reads" every time they pass an RFID reader, in the process generating information about an individual's movement in the real world. It is not unrealistic to therefore suggest that RFID tags are cookies for the real world.

The majority of prior research on RFID deployments addresses how RFID can be used to create information about things in the real world. However, RFID is also used to create information about people in the real world. Some people tagging is direct and purposeful, but people can also be tagged indirectly by tagging the goods that they carry around with them, or are responsible for moving. Because of the possibility of tagging individuals, one of the most interesting developments in RFID is the potential for using the technology to generate information that can be used to monitor the provision of services by contractors. Given the extensive and growing proportion of outsourced contracting undertaken by the DoD (U.S.

Department of Defense) and other militaries around the world, it is therefore timely to consider the use of RFID technology for monitoring contractors.

Throughout the paper I assume the reader has a basic knowledge of RFID technology, the economics of monitoring, and contracting for services by the military. I will not spend any time at all describing these issues, and will instead focus on the empirical case studies and survey results. Readers who wish to acquire a basic knowledge of RFID might find it useful to refer to Sweeny (2005) and Wyld (2005). The economic literature on monitoring is enormous, but among the many contributions on this topic the work of Alchian and Demsetz (1972) is widely regarded as seminal. Service contracting by the military is the topic of an excellent recent book by Singer (2003).

The paper proceeds as follows. Section one explains the basic intuitions behind the suggestion that RFID might be used for contractor monitoring. Section two uses a multi-case study methodology to investigate the application of RFID to monitoring human subjects in a variety of domains; the objective here is to understand the current use of the technology and induce from this some understanding of the circumstances under which RFID might be used for contractor monitoring. This is follows by Section three, which investigates the privacy implications of monitoring individuals with RFID. It uses an internet survey to gather data on privacy preferences among subjects that might be tagged, and applies adaptive conjoint analysis to investigate the results of the survey. Conclusions round out the paper.

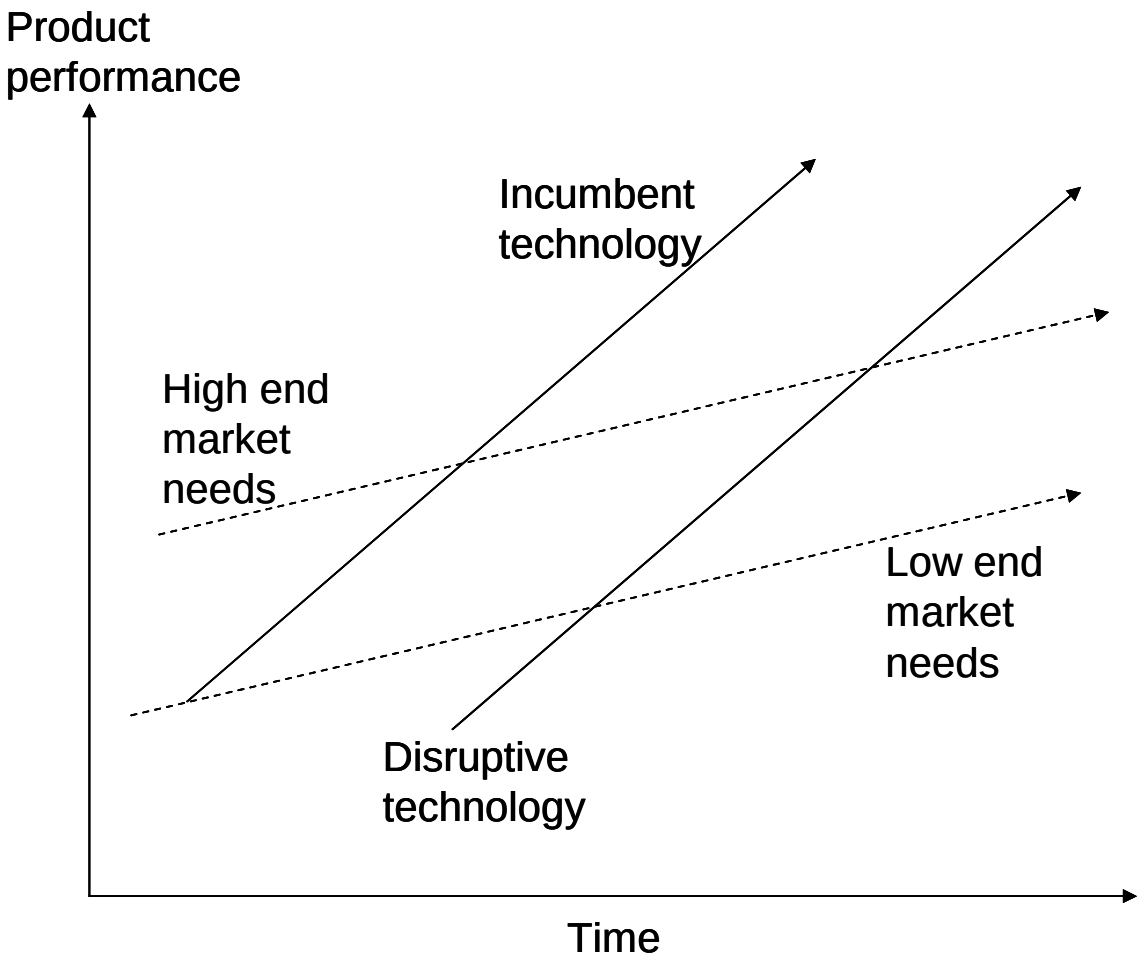
THIS PAGE INTENTIONALLY LEFT BLANK

SECTION I: SOME BASIC INTUITIONS ABOUT THE OPPORTUNITIES FOR APPLYING RFID TO THE PROBLEMS IN CONTRACTOR MONITORING

Understanding RFID as a disruptive technology

In recent years a successful academic mini industry has addressed the question of the emergence of new technologies that disrupt existing technologies (Christensen, 2000; Danneels, 2004). A classic example of a technology with the characteristics of a disruptive innovation was steel mini mills. Initially, mini-mills emerged at the very bottom of the steel market, barely able to meet the quality requirements for rebar, a poor quality steel used in building construction. As a result, mini mill technology was of no interest to major steel producers, who used superior smelting processes that produced high quality steel with high margins. However, mini mills were cheap to build because of their small scale, which was appealing to upstart entrepreneurial firms such as Nucor and Chapparel. These firms steadily improved the quality of steel produced by mini-mills, which remained low cost. Therefore over time, mini-mills penetrated higher quality steel markets, disrupting traditional steel making technologies as they went. Diagram 1 illustrates this process:

Diagram 1: Technology Trajectories (Christensen, 2000:xvi)



A good way to understand the general agenda of this paper starts by placing RFID within this basic framework, and considering the possibility that RFID might be a disruptive technology (an idea considered by one of Christensen's collaborators, see Raynor, 2004). We are already seeing that RFID is disruptive of GPS (global satellite positioning) devices in some applications, i.e. some RFID applications involve RTLS (real time location monitoring) as a cheap substitute for GPS. It currently has lower performance than GPS and has found an initial customer base in market segments that are marginal to mainstream GPS (ex: automobile distribution processes), consistent with the pattern observed for disruptive technologies.

In this paper I consider the possibility that RFID might be disruptive of various traditional contractor monitoring technologies that are currently employed by DOD. There are two key issues to bear in mind when making a realistic assessment of the possibility that RFID might emerge as a disruptive monitoring technology. The first is that the value proposition of disruptive technologies is completely different from incumbent technologies (Christensen, 2000:32-33). Disruptive technologies often emerge completely outside the mainstream market, looking like there is no way they will ever adequately serve mainstream market needs. However, over time, they come more and more able to perform in ways that meet the key demands of higher end customers, as illustrated in Diagram 1. The basic intuition here is that disruptive technologies initially are unlikely outsiders, but evolve faster than customer demands, so they eventually becoming adequate enough in the eyes of customers that customers switch from the incumbent technology to the upcoming (disruptive) technology.

At the current point in time, it seems a little imaginative to suggest that RFID might have widespread application as a contractor monitoring technology. However, as the case studies in this paper amply illustrate, some organizations are already using RFID in a variety of ways that involve direct monitoring of human subjects. This is completely consistent with how disruptive technologies emerge, initially in non-mainstream applications where they evolve and develop, becoming adequate for launching a successful attack on mainstream applications by this process. It is to be noted that many privacy activists seem to see the potential for RFID to be used as a pervasive human subjects monitoring technology, and are alarmed by the rate of improvement in RFID technology as well as in other elements of the RFID system of innovation, such as software that helps sort all of the data generated by RFID into usable form (Dew, 2006). This indicates that at least some stakeholders in RFID already see its disruptive potential.

The second key issue to bear in mind when making a realistic assessment of the possibility that RFID might emerge as a disruptive monitoring technology is that

pervasive uncertainty surrounds the evolutionary development of innovations. In this regard, a particularly fine paper by Nathan Rosenberg is worth quoting at length:

> I would like to begin with two generally accepted propositions: First, technological change is a major ingredient of long-term economic growth, and second, technological change is characterized by a high degree of uncertainty. Understanding the nature of these uncertainties and the obstacles to surmounting them is not a trivial matter. Rather, it goes to the heart of how new technologies are devised, how rapidly they diffuse, the ultimate extent of that diffusion, and their eventual impact on economic performance and welfare.
>
> In view of the great uncertainties attached to the innovation process, it is hardly surprising that innovating firms have, historically, experienced high failure rates… But to describe the high failure rate associated with past innovation is to tell only a part of the story, and perhaps not the most interesting part. Indeed, I want to suggest that *the more intriguing part of the story… has been the inability to anticipate the future impact of successful innovations, even after their technical feasibility has been established.* This statement remains valid whether we focus on the steam engine 200 years ago or on the laser within our own lifetimes. (Rosenberg, 1996:91; italics added).

With an eye for historical generalizability, Rosenberg goes on to delineate three key uncertainties about innovations: first, an inability to predict the relative rate of improvement among rivalrous technologies; second, an inability to predict key complementarities among technologies (i.e. technologies can be analyzed as interdependent systems where the performance of the whole depends on innovations in the subsystems), and; and third, an inability to predict changes in consumer demand. For all three of these reasons, Rosenberg points out that to map the history of innovation is to map a history of great uncertainties.

Rosenberg's point is that even when the technological feasibility of an innovation is proven – as it surely is for RFID – still few of the consequences of the

innovation in use are foreseen. My job in this paper is therefore to attempt to pierce the fog of uncertainty just a little, in order to evaluate some of the possibilities of utilitizing RFID as a contractor monitoring technology.

RFID possibilities as a monitoring technology

The intuition that RFID might have some effective applications in contractor monitoring arises from several different observations about the possible role of this technology given prevailing theories and practices. I have grouped these observations into four categories, as follows: first, mitigating post-contractual opportunism; second, substituting human monitoring; third, forensic analysis; and fourth, introducing contract alternatives. The following sections of the paper explain each of these categories in more detail.

1. Mitigating post-contractual opportunism

Information asymmetry is the central feature of a principal-agent models. In such scenarios the individual contracting for a service (the principal) commissions another individual (the agent) to act on its behalf. However, the principal has incomplete information about the agent's exact goals and behavior (referred to as an information asymmetry). Therefore, at least in principle, technologies that generate information about the behavior of agents might reduce this information asymmetry by making the agent's actual behavior visible to the principal. This might be valuable to the principal because it seeks to ensure that the agent performs tasks according to the principal's requirements, given the contract terms agreed between the principal and agent. Moreover, agents would modify their behavior because of the knowledge that they are being actively monitored by principals, and that this monitoring has reduced the asymmetry in information between agent and principal compared to the scenarios where no technology is used. This argument straightforwardly suggests that there may be some applications where RFID tagging of individuals is value-creating.

Empirical data confirms that over-billing and short-changing on contract terms are endemic in contracting, including in military contracting where firms (agents) are

tempted to increase their profits at their client's (principal's) expense, just as they are in any other scenario. According to Singer (2003:155):

> Private businesses have cheated public agents during war extending back to the Philadelphia merchants who swindled the Revolutionary Army while it starved at Valley Forge. The privatized military industry simply represents a new manifestation. Now the cheating is also an opportunity on the services side, instead of overcharging for goods.

Singer goes on to catalog several well-known examples of what economists refer to as "ex-post rent extraction" or "opportunism" by firms, i.e. over-billing or short changing their clients after the ink has dried on their contracts, including "padding" staff numbers with "shadow" employees (p.156), citing data from the GAO (General Accounting Office) among others (p.157). DynCorp and BRS are both cited by Singer; more recently BRS has also been investigated for over-billing on contracts in Iraq.

One obvious way of ensuring that you get more of what you pay for is to effectively monitor the provision of services with technology. RFID is one technology that is suited to such applications. For example, a RAND study on RFID in the workplace (Balkovich et al, 2005) found that some firms are using RFID-generated information to police working hours rules in white-collar office environments, i.e. collecting precise data on employee attendance. Some universities have also started using RFID to automatically collect data on class attendance by students (more on this later in the paper). These and other examples comprise proof-of-concept that RFID tagging might be used to precisely monitor the presence of agents on site, including the activity of agents by tracking their movement around sites.

At first sight this seems like a very mundane use for a sophisticated technology, but initial impressions underestimate the powerful surveillance potential of RFID (Stepleton-Grey, 2005). A system of distributed RFID readers is a powerful way to invisibly oversee the whereabouts and activities of individual subjects in any particular location. Furthermore, RFID tags can be equipped to include motion

sensors and other devices that add additional surveillance potential to basic identify/location features.

2. Substituting human monitoring

A second intuition about the potential role that RFID might have some contractor monitoring applications arises from shifts in the relative prices of labor versus technology. In short, RFID is getting much cheaper (and its costs are more predictable), whereas labor is getting steadily more expensive (and future fully built-up costs are less predictable). Although the pace of relative change in these cost variables remains to some extent uncertain, the general direction of the trend is sufficiently clear that it is possible to say that RFID monitoring is likely to steadily substitute monitoring by human subjects.

There are additional reasons why this trend is likely to be especially important in military environments. First, the military currently faces enormous pressure to reduce its immediate overall manpower requirements, both in order to reduce its total budgeted costs, and to adjust to lower recruitment levels. These pressures to generally reduce manpower requirements have the consequence that back office staff (the kind that normally would be involved in monitoring contract compliance) are being steadily reduced, even as the contract supervision workload is steadily increasing. This creates a gap in the military's ability to monitor contractors. One logical means of filling this gap is to use available technology, such as RFID. Even if the information created by the technology is rudimentary in its current state of development, it creates an auditable data trail. Manpower-related pressures serve to overcome some of the inertia that normally accompanies the adoption of new technologies in large organizations such as the DoD, and in particular the resistance to adopt technologies that may initially seem to under-perform on some metrics (more on this in the conclusion to this paper).

Second, given the business military organizations are in, the safety and security of all staff has to be taken into account. Despite the obvious need for contractor monitoring in dangerous and unstable environments (take Fallujah, for

example) there are equally obvious reasons for minimizing the number of personnel involved in any kind of monitoring activities is these danger zones. As the threat to the safety and security of personnel increases, the costs of maintaining adequate safety and security increase, and these costs have to be traded-off against the value that can be gained by actively monitoring contractor activities. It is probably not just coincidence that some of the charges of contractor opportunism (such as recent ones against subsidiaries of Haliburton working in the Fallujah area) occur in areas that are dangerous and unsavory places to go just to ensure contractors are delivering on their contracts. Contractors understand these trade-offs very well, and may take advantage of them (i.e. behave opportunistically). Once again, even if the information created by RFID technology is rudimentary in its current state of development, it creates an auditable data trail that is better than no data at all in reducing the costs of opportunism.

As a result, RFID is one of a suite of technologies that may be favored by military units with responsibility for contractor monitoring in order that some form of monitoring may be done remotely, from safe and secure locations. This is no different from security guards using sensors, access systems and video surveillance to monitor building security from remote locations.

3. Forensic analysis

Using RFID for forensic analysis refers to the post hoc use of data gathered by RFID systems for investigative purposes. According to RAND (2005:12), "a typical use might be investigation of asset theft or of compliance with company timekeeping policies." Following from the previous section, where I highlighted the often rudimentary nature of RFID data, even if the information created by the technology is rudimentary it creates an auditable data trail. The important point that follows from this is that it enables exception monitoring to be conducted on a post hoc basis, and this in turn enables the threat of contract monitoring to be made credibly. Even if most contracts are not monitored, a credible threat of monitoring will be sufficient to enforce compliance, up to a certain point. In principle this is no different from any other form of policing. For instance, criminal enforcement relies

on the threat of being caught (probabilistically) rather than on penalties of certain detection. However, once a suspect is in hand, forensic data can help enormously in prosecuting a case just because ex post an individual's behavior can be reconstructed from a variety of data. In the same way, RFID can provides a rudimentary data trace that can be valuable for forensic purposes, just as the RAND study highlights.

To illustrate the power of RFID in forensic applications, consider the following example. Sysco, the largest distributor of temperature-controlled food, is testing a semi-passive RFID system to identify, locate and track individual trailers as they move through the supply chain, and to monitor and record at regular intervals the temperature conditions inside refrigerated trailers. Upon delivery, the tags are handed to the customer, who can then interrogate them to inspect the temperature log before accepting the shipment. Temperature monitoring supports quality by assuring the customer that the goods were kept at the correct temperature through the supply chain. Ultimately, this also saves costs by providing the ability to detect which party was responsible for losses; this, in turn, reduces the costs of moral hazard and reduces insurance premiums.

Because post hoc forensic analysis can only be done if relevant data has been collected, it may make economic sense to utilize cheap technologies that capture data on a range of variables, even if the data is only used on a contingent basis. This kind of contingent application of RFID is most powerful when different kinds of data about contractor performance is captured and linked to other variables in the course of investigation.

4. Introducing pricing alternatives

The final potential role for RFID in contractor monitoring applications that I highlight here arises from RFID's capability of generating numerous new measures of processes. Measurement data has value because the rational design of contracts depends on costs of measurement (as well as bargaining and enforcement, as outlined in transaction cost economics – see Coase, 1937; Foss and Foss, 2005).

Because RFID introduces cost-effective alternative means of measuring activities (such as assembly processes or the consumption of services) it therefore may create value by allowing contracts to be measured more efficiently by the principal or redesigned in ways that are more efficient for the principal (i.e. DoD).

An example of RFID's potential as a measurement system – and the re-pricing opportunities that come with that – is Michelin's use of semi-passive RFID tags for smart tires. Smart tires allow leasers to identify individual tires and monitor tire operating conditions such as distance run, pressure and temperature at regular intervals, thus accumulating historical data on tire use. For the tire owner, this helps the enforcement of tire-leasing contracts by collecting information on tire abuse by users of the tires. Consequently, smart tires bring a number of benefits to vehicle fleet operators and tire owners. They are easier to manage since RFID helps in the development of fair tire leasing contracts with efficient consumption measures. This data tracking reduces the conflicts between supplier and buyer by ensuring that the tires operate at proper parameters.

Because the relative cost of negotiating/enforcing versus measuring, the optimal mix of contract provisions would almost certainly change if cheap RFID-based measurement technology was widely available. Changes in relative measurement costs would make some contract types look more attractive versus alternatives, and therefore the equilibrium mix of contract provisions would change. This trend is already emerging in the insurance industry, where auto insurance companies are piloting Pay-As-You-Drive insurance schemes that replace annually priced insurance contracts with monthly variable-price contracts.

SECTION II: RFID AS A MONITORING TECHNOLOGY: CASE EXAMPLES

Where did the idea of directly tagging people come from?

RFID technology has evolved over many decades to the point where it is currently emerging as a general purpose identification technology used in a very wide range of applications. The idea of tagging people directly can be traced through two evolutionary pathways: animal tagging and entry systems.

Animal tagging

Like several other significant technologies (high performance avionics, integrated circuits, computer software) many of the important research and development breakthroughs for RFID were sponsored by branches of the U.S. government. In the mid 1970s the USDA (Department of Agriculture) asked LASL (Los Alamos Scientific Laboratory) to develop RFID tagging to identify and track livestock (initially cattle). The problem the researchers were asked to tackle was how to identify cattle so that the animals could be given hormones and medicines (Roberti 2005). LASL came up with low frequency (125 khz) passive RFID tagging system that used a transponder encapsulated in glass that was injected into cattle, i.e. subcutaneously. In the U.S. commercialization of this technology was spawned by the transfer, in 1977, of government-developed technology through LASL initially to two private firms: Amtech and Identronix (both of which survive as subsidiaries of larger firms). Cattle tagging subsequently became one of the first major markets for RFID (mainly in Europe, more recently in the U.S., following the BSE scare in 2004). This later evolved into tagging other animals, including household pets. Rice grain size implantable microchips identify over one million pets in the U.S., and over 10 million in Europe.

Unsurprisingly, it was only a matter of time before subcutaneous RFID implants in human subjects started to appear, initially using tags originally designed for pets. At least one implantable RFID device has received FDA approval and there

have been several high profile articles about tagging human subjects with subcutaneous RFID tags. I will not describe any of these applications in detail here, but the reader should be aware that these tags are already being used for security-oriented applications.

Entry systems

A second direction from which RFID tagging of human subjects emerged is entry systems. The path of evolution here was from key-based systems, through magnetic stripe cards, and onto RFID-based contactless cards used in entry systems. According to a study by RAND (Balkovich et al, 2005) these systems have been in use since at least 1995. In fact, the original application patent for RFID-based entry systems was granted in 1973 to Charles Walton, who received a patent for using RFID to unlock doors and subsequently licensed it to several firms. As microchips costs declined in the 1990s, applications for RFID began to spring up in access systems for office buildings and keyless entry systems for cars (which made up approximately half of worldwide deliveries of RFID transponders in 2000). It is now commonplace for office entry systems to feature RFID-enabled identification badges and key chains.

Case studies of RFID applied to human subjects monitoring

In this section of the paper I use the same multi-case methodology as used by Apte et al (2006), i.e. a multi-case study that aims to discover how RFID is already being used in applications that involve directly or indirectly tagging individual human subjects.

The logic behind this multi-case methodology is that there is substantial variation in RFID applications and the use of RFID technology in business/military applications is quite recent. This makes case research an appropriate methodology to use in the context of investigating the relationship between RFID and a new topic of interest: contractor monitoring. This methodology lends itself well to early, exploratory investigations where the variables are still unknown and the phenomenon not well understood. As argued by Meredith (1998), an emergent

phenomenon can be studied in its natural setting with case research, and a meaningful, relevant theory can be generated based on the understanding developed through observing actual practice.

When building theory from case studies, it is possible to select cases using alternate approaches of sampling or replication. (Eisenhardt, 1989; Yin, 1994). Since the goal of the research at hand is to develop practical / managerial guidelines for the possible use of RFID technology in the domain of contractor monitoring, I use the former approach to understand how RFID is used for human subjects tagging across a spectrum of applications.

Cases were selected as follows. I started with a database of public sources of information on RFID which encompasses several thousand documents collected in the 2002-2006 period. From this database I initially screened 27 possible cases that involved direct human subjects tagging (rather than object tagging, which is a much more common application of RFID). Out of this subgroup, I then selected 6 cases for detailed study, based on their appropriateness for exploring the possibility of RFID-based contractor monitoring. Table 1 details the 27 cases screened and identifies the 6 cases selected for further study with a * and highlighting.

Table 1: RFID cases screened

Tracking applications
* Aircraft manufacturing: assembly tracking tag
* Student tracking: recording class attendance
* Timekeeping tags for sporting events
* Tracking grocery store shopper behavior
Manufacturing plants: clocking in and out
Vehicle entry systems: Fedex RFID wristbands
Semiconductor manufacturing: tagged bunnysuits
MountainWatch ski resort tagging
Security applications
* Inmates tagging in prisons
Home arrest tags
Office entry systems
Identifying critical people: subcutaneous human tags (Mexico)
School kids anti-abduction tags
Theme park tags: Legoland kids “lost and found” tagging
Mine and tunnel worker tagging
Oak Ridge Evacuation and Rescue system
BP Cherry Point refinery worker tracking (emergencies)
LKAB (Sweden) iron ore mine worker tracking (safety during blasting)
Medical applications
* SARS patient tracking tags (Singapore)
Hospital visitor tags
Navy medical dogtags (TACMEDS)
“Digital Angel” subcutaneous identity tag for elderly
Verichip implants for accessing medical records
Newborn anti-abduction systems
Patient tags: Alzheimer’s patients access control tags (Japan)
Mortuary tracking bodies (post Hurricane Katrina)
Convenience applications
Implanted tag for wallet-less payments (nightclubs in the UK, Spain, Mexico)

Case 1: aircraft assembly processes

Lockheed Martin has been using RFID to track aircraft assembly work for several years at three of its plants (Dallas-Fort Worth, TX, Marrietta, GA and Palmdale, CA). It does this by placing RFID smart-card readers on manufacturing equipment and workstations throughout its plants. Before a worker uses any of the equipment they must use their RFID-enabled ID card to authorize access to the

equipment. A computer system then records every authorization event as a transaction, and keeps a record of all of the processes performed by the employee using the equipment.

One reason Lockheed switched to the RFID-enabled system is that it removes redundant tasks for workers and thus promotes efficiencies. For instance, workers used to have to swipe their magnetic stripe cards through a reader; with the RFID system they only have to wave the card close by the reader. This removes actions that do not add value in the assembly process. At the same time, the RFID-enabled system allows Lockheed to remove many manual record keeping processes that required human interventions, thus substituting electronic records for manual ones.

A second reason Lockheed adopted RFID was for quality assurance purposes. Given the type of manufacturing the firm is involved in, it is critical that it (the agent) can closely monitor the assembly process to ensure its customers (the principals) that work was performed to specification, i.e. to be able to provide data that proves quality. For example, Lockheed assembles kits that go into the production line for aircraft that have in the range of 20-100 sub-components and may be customized “one offs”. Because the opportunity for mis-assembly is large, very detailed monitoring of the assembly process is necessary.

Case 2: SARs patient tracking in Singapore

When SARS (Severe Acute Respiratory Syndrome) broke out in the Far East in 2003, two Singapore hospitals started using RFID tagging in order to track visitors, patients and staff, so they could trace all of the people with whom a suspected SARS patient has had contact.

The system worked by issuing identity cards embedded with an active RFID tag with a small battery to patients, visitors and staff. Everyone issued with a card had to register their name and contact information in case it was necessary to contact them later. RFID readers were placed around hospital facilities, which were divided into zones, with one reader in every zone.

The purpose of the system was to allow instant forensic analysis to be done: if a patient was suspected of having SARS, staff were able to run an instant check of who else had contact with the patient, where and when. The system stored all this data for 21 days which was thought to be long enough based on the fact that SARS has an incubation period of 10 days. For confidentiality reasons, the data was deleted after that period.

Besides its forensic analysis capabilities, another benefit of the RFID system was the ability to track everyone in the hospital without requiring manual staff intervention, i.e. the system substituted human monitoring processes.

Case 3: Timekeeping in sporting events

Starting with the Boston marathon in 1996, RFID has become a standard measurement technology for sporting events around the world. Literally thousands of athletic events have used RFID tags attached to runners' shoes to time participants in marathons and other sporting events in every corner of the globe, from Beirut to Bangkok to Boston. Skiers have also been tagged, including participants in the 2002 Winter Olympics.

From 1999 Boston marathon organizers began enabling friends, family and other spectators to monitor the progress of runners on the Internet, as well as accurately time them for official race purposes. Every runner has an RFID tag tied into the shoelaces. The tag contains a unique ID assigned to that athlete, and when they runs over RFID-receiving mats on the raceway the system logs the runner's time at that point into a database.

Given this information, race organizers can track the progress of runners and even forecast when they will finish the race, based on information about time differences between when each runner crosses the mats.

This information is also made available to the press and public. Boston marathon organizers even arranged for 75 volunteers to wander the crowds with wireless PDAs (personal digital assistants) answering questions and provide location

information to spectators. Friends and families of runners could log onto the Internet, check times and even set up an automatic alert based on the predicted time a friend is going to finish the race. More than 180,000 alert messages were sent in 2002, the first year the system was available, and in 2004 the system served up more than 7 million web page views.

Case 4: RFID in prisons

RFID has emerged as a popular technology for tracking the movements of inmates in prisons. Calipatria State Prison, CA was the first jail in the U.S. to adopt RFID tracking for inmates in 2000. Since that time correctional facilities in Michigan, Illinois and Ohio have also adopted the technology for 3,000 inmates. In 2005 the Los Angeles County Sheriff's Department launched a pilot covering 1,800 inmates, with plans to eventually apply the technology across the whole county, covering 18,000 inmates.

RFID inmate monitoring works by issuing every inmate a bracelet that has an active RFID tag embedded in it. The bracelet carries the inmate's identity number and is referenced to personal information contained in the prison's database, including data that "profiles" the inmate along certain dimensions, i.e. restricts him/her to certain parts of the jail, sets up "keep away" alarms from other particular inmates, etc. The bracelet sends out a RFID signal every two seconds, and includes tamper-proof safeguards such as a braided stainless steel wire that runs the length of the bracelet (if cut the tag stops transmitting, which triggers an alarm) and a skin contact sensor (if removed for more than 15 seconds, this also sets off an alarm).

Readers through the prison complex continuously log signals received from inmates' bracelets and rely this data to a control center where prison guards monitor inmate behavior on a screen depicting the floor plan of the facility. This allows guard to pinpoint the location of staff and prisoners in real-time within the facility. Officers can monitor inmate movements, including congregations of up to 20 inmates. Guards wear bracelet's that also have an emergency button on them to set off a rescue call.

The inmate tracking system is thought to have several benefits in addition to its chief purpose of protecting correctional officers: prison costs are reduced because inmates know they can be placed at the scene of an incident, such as theft, property damage, violence against other inmates and escape attempts.

Case 5: student class attendance

Several examples exist of RFID being used in schools and universities to monitor students for either security (kidnap prevention) or attendance monitoring. One example is the RFID system tested at Brittan Elementary School in Sutter, CA in 2005. The school tested a system that automates attendance-taking by placing RFID readers on classroom doorways and giving students passive RFID tags with a unique 15 digit identity number embedded in student identity cards. The system was of interest to the school district because California bases school aid upon attendance numbers, which puts a priority on fast, low cost, reliable monitoring of student attendance. The idea was that RFID monitoring could decrease the amount of time teachers spend taking attendance manually.

As piloted at Brittan, the system kept a record of students present, absent and tardy, based on the student's time of entry into the classroom. This data was wirelessly uploaded to a PDA issued to the teacher, who then performed a quick visual check to verify class attendance. Once confirmed, the list was then electronically filed with school administrators, and from there to the state board of education.

Japan and the U.S. have led the adoption of RFID for student tracking. However, the Brittan initiative and others like it have been shelved after nationwide media attention on the issue of privacy invasion (a subject we will return to later in this paper).

Case 6: tracking shopper behavior

One novel use of RFID for tracking human subjects involves tracking shoppers' traffic patterns in grocery stores, which has been undertaken by at least one retail market research firm in 20 stores throughout the U.S. since 2001.

Using an RFID technology known as RTLS (real time location system) every grocery cart in a supermarket had an active RFID tag placed on it. The tags emit a signal once every five seconds, which is received by RFID readers in the store, which triangulate the precise location of the cart and therefore track the grocery cart's route through the entire store, using the cart's path as a proxy for the actual shoppers' path. The result is an in-store version of GPS (global satellite positioning) system.

The data is then aggregated, visually mapped and statistically analyzed in order to understand typical shopping patterns (Larson et al, 2005). Retailers have long-standing beliefs about how consumers move around stores, i.e. ideas about how customers move around aisles, promotional displays and the perimeter of stores. However, Larson et al's (2005) analysis of actual shopper patterns challenges many long-standing perceptions of shopper behavior, including:

- The belief that grocery shoppers weave up and down all aisles: instead, most shoppers actually travel select aisles.
- The belief that shoppers shop a whole aisle: instead, most shoppers actually do short excursions in and out of select aisles.
- The belief that the perimeter of a store (nicknamed the "racetrack") was only visited as a way of getting access to the aisles: instead, the racetrack is actually the main thoroughfare of the store.

This method of monitoring shopper movements represents a significant step forward in understanding the shopping paths taken by individual shoppers in actual stores, with potentially important implications for overall store design as well as the placement of sale items, etc.

Synthesizing the case studies

The basic message that arises from these six case studies of RFID applications is that direct human subjects monitoring using RFID is actually already happening in several different ways, and that the value of monitoring is derived along at least four dimensions, as outlined earlier in this paper: by mitigating opportunism, substituting human monitoring, through forensic analysis, or by generating new processes measures upon which contract pricing alternatives can be based. These dimensions are tabulated in Table 2 (on page 31) along with other key characteristics of the RFID technologies considered here.

While no one classification scheme can adequately describe the key characteristics of a technology, multi-case studies like the one presented here – when combined with other studies of a similar kind (see Apte et al, 2006) - help to generate new knowledge about RFID by providing taxonomies that are useful for practitioners who want to understand how RFID might be applied, as well as being useful for academics who seek to understand the underlying drivers of value of a technology in applications.

A complimentary way of illustrating the potential value of RFID monitoring is through analogy.

Take the example of shopping carts, for instance. What reason do we have to believe that there is any less "widely accepted folklore" (Larson et al, 2005) about contractor behavior than there is about shopper behavior? If RFID tagging of shopping carts can help reveal empirical data on true shopper behavior, isn't it also at least plausible to think that it can help reveal empirical data on true contractor behavior?

Next, taking the example of tracking marathon runners. If it is possible to create a low cost way of timing athletes in sporting events, and make that information available wirelessly to a PDA and through the internet, why wouldn't there also be value in applying the same technology to contractors, and make the information similarly available to a large number of potential monitoring agents. This

would a) make it more likely opportunistic behavior was detected, and b) create social pressure not to behave opportunistically, which is a well-known effect of "publishing" behavior. Couldn't the same technology be applied to the problem of "who's watching the nightwatchman?"

To take a third example, consider the role that monitoring plays in changing the behavior of prison inmates: prison costs are reduced because inmates know they can be placed at the scene of an incident, such as theft, property damage, as well as violence against other inmates and escape attempts. In principle, are not exactly the same monitoring benefits available to discourage the worst abuses DoD property and equipment by contractors? If RFID bracelets are useful for ensuring that inmates do not "double dip" in the cafeteria, isn't it also possible that it would be a useful way of making sure that contractor's don't double dip the DoD, in whatever form that might take?

The point here is not to suggest that DoD contractors are all crooks, and should be treated like inmates. Instead, the point is exactly the one that Williamson (1985) famously made about opportunism: the monitoring problem exists not because every agent will cheat, if possible; instead, it exists because ex ante the principal does not know which agents will cheat; therefore monitoring must be done with an eye to deterring cheating among all agents. That may mean that RFID can play a role in increasing contracting efficiencies.

Table 2: summary of RFID case studies

	Aircraft assembly tag	**SARS patient tracking**	**Sport event timekeeping tag**	**Prison inmate tagging**	**Student attendance tracking**	**Shopping carts**
Chief applicability to contractor monitoring issues						
Mitigating opportunism	*				*	
Substituting human monitoring	*	*	*	*	*	
Forensic purposes		*		*		
Pricing alternatives			*			*
Tag characteristics						
Tag type	Passive	Active	Passive	RTLS	Passive	RTLS
Frequency	LF 125 khz	UHF 433 mhz	HF 13.56 mhz	UHF 900 mhz	UHF 915 mhz	UHF 433 mhz
Read distance	Short (a few inches)	Long (over 30 feet)	Medium (a few feet)	Long (over 30 feet)	Medium (a few feet)	Long (over 30 feet)
Information richness	Low: ID number only	Low: ID number only	Low: ID number only	Low: ID number only	Low: ID number only	Low: ID number only
Form factor / size	Embedded in ID card	Pack of gum	Large postage stamp	Large wrist watch	Pack of gum	Pack of gum
Attachment	Worn as badge	Hung around neck	Tied to shoe	Secured to wrist	Hung around neck	Fixed to trolley

SECTION III: WILL THEY WEAR IT? – PRIVACY ISSUES

Any realistic assessment of the prospects of RFID as a general purpose monitoring technology must take into account the obstacles to monitoring people, i.e. privacy invasion. Therefore a large part of the research that this paper reports on has involved exploring this issue empirically through an internet survey that used conjoint analysis to find out how much value individuals place on their privacy.

The practical importance of this issue struck me during a meeting with SAVI technologies. SAVI executives commented that in Iraq truck drivers routinely use bolt cutters to cut off RFID tags from supplies they are transporting, for fear that the RFID device might be used by insurgents as a trigger for improvised explosive devices (roadside bombs) or might act as ready-made homing devices for shoulder-fired missiles. What this anecdote highlighted was the fact that all RFID tagging of human subjects relies on a hidden assumption: that people will wear the tags. However, particularly in military contexts, this assumption may be false.

Privacy issues raised by RFID technology has in fact been the focal point of much recent public debate. I will not delve into this debate in great detail here, as I consider it outside the scope of this study. Instead, I simply highlight the following points:

- Two major books on RFID privacy issues were published in 2005: Simson Garfinkel's "RFID: Applications, Security, and Privacy" (Garfinkel and Rosenberg, 2005) and Katherine Albretch's "Spychips" (Albretch, 2005).
- The December 2004 edition of Harvard Business Review carried a case study on RFID privacy issues
- RAND completed a study of RFID in the workplace in 2005 (Balkovich et al, 2005)
- The GAO (General Accounting Office) issued a report on RFID privacy issues in May 2005 (GAO, 2005). Among other points the report made, it pointed

out that legislation on privacy issues relating to RFID was under consideration in six different states.

- In March 2005 Benetton was the target of a successful boycott after announcing it planned to introduce RFID tagging on some of its clothing. The firm was forced to withdraw its plans.
- Some large corporations – among them Proctor and Gamble being most prominent – have appointed "Privacy Officers" to their executive boards.
- In the Fall of 2005 the General Workers Union in the U.K. announced the results of a study conducted by the University of Durham (U.K.) which found that hundred of thousands of logistics workers were already being indirectly monitored using RFID. The union called for an immediate ban of such monitoring and began proceedings to take the issue of RFID monitoring through the European Community legal process, with the aim of having the technology banned.
- At a broader level, RFID monitoring is just one aspect of wider concerns about information privacy which have been raised by the Internet. Beyond this, there is a long history of constitutional safeguards in the U.S. and other countries that protect individual's rights to privacy, as well as an extensive literature on privacy-related topics in philosophy, politics and economics.

Perhaps because RFID is still emerging as a mainstream technology, it seems that there is little research-quality empirical data on RFID and privacy issues (though there is a research literature addressing general privacy issues – for example Acquisti and Grossklags, 2005; Camp and Lewis, 2004; Stigler, 1980). Given the obvious importance of the privacy issue in any practical contractor monitoring application of RFID, I therefore decided to create a survey instrument that would allow some analysis of individual preferences for privacy in the workplace.

The survey

An Internet-based survey instrument was used for data collection (the complete survey can be viewed online at http://www.imdresearch.ch/id_survey/). The survey was in two parts:

- o Part 1 collected descriptive data on participants, covering commonly collected demographic variables such as gender, group affiliations, military rank, etc.
- o Part 2 presented respondents with a fictitious (though realistic) military ID (identification) system, and asked respondents to rate how desirable it would be to be able to use the proposed ID system in certain ways – for example, ranging from "Not Desirable" and "Somewhat Desirable" to "Very Desirable" and "Extremely Desirable".

The survey instrument was "adaptive" in the sense that early responses "channeled" respondents into relevant future questions, rather than having every respondent fill out every aspect of the survey (this economizes on respondents' time and eliminates redundant data). The survey was designed and administrated by two marketing research experts at the IMD business school in Lausanne, Switzerland.

The sample used for this study was 55 students enrolled in defense-oriented resident and executive MBA programs. Participation was anonymous. Nearly all respondents had military careers. 28 students responded, giving a response rate of approximately 50%. It should be noted that the sample was a "convenience" sample made up of career military individuals rather than contractors. Therefore, while there are some reasons for thinking that the basic demographics are representative of contractor demographics, caution must be exercised in interpreting the results of the survey since there may be systematic differences between this sample and a representative sample of DoD contractors. This issue clearly should be subjected to further empirical study.

The procedure followed in administrating the survey was as follows. First, we created a test survey featuring an RFID-tagged pharmaceutical product in order to examine the potential impact of RFID on privacy. Given the initial results of this survey, we developed a new survey specifically oriented to military ID tagging in the workplace. We sent the sample of respondents a short email requesting their participation in a survey, with a link to the survey website embedded in the email for their convenience. We estimate the survey took approximately 20 minutes for each respondent to complete. A week after the first email, we sent a follow-up email,

again requesting participation. The number of completed surveys was based on these two solicitations only. Participation was voluntary; no rewards were offered.

We analyzed the survey results using common statistical methods. Subjects' overall ranking of features of the ID tag system (relative utility levels) were as follows:

Table 3: summary survey data

Keeping record of presence through your ID	7.50
Entry and access through ID system	9.63
Flexibility in choosing features	11.59
Form of the ID system	11.64
Ability for others find you through your ID	12.13
Use as a payment system	14.28

The **first** result that appears from the survey is that the least preferred feature of the ID tag system was keeping a record of an individual's presence through the ID system, which is exactly what an ID tag for monitoring individual behavior is designed to do. Importantly, this confirms the intuition most people have that tracking individual movement for "business" purposes conflicts at some basic level with individual preferences for privacy. The most preferred feature of the ID tag was the ability to use it as a payment system, a feature that benefits the tag wearer (the employee, or contractor), not the employer. The relative ranking of other features lay in between these two extremes. For practicing DoD managers these results suggest that ID tagging policy needs to be formulated with an eye to the possible "benefits" (to contractors) as well as the "costs" (in terms of privacy invasion). ID tags could be made much more acceptable to contractors if they are "packaged" as a combination of features, rather than simply as a tracking device.

Within these overall results, we asked additional questions about more specific features of the fictitious ID system. In the following Table, more detailed survey results are presented.

Table 4: detailed survey results

Keeping record of presence through your ID		
Time Period	*Location*	
Working Hours	Immediate Workplace	9.36
Working Hours	Any work-facility	3.55
After-work hours	Immediate Workplace	1.76
After-work hours	Any work-facility	1.86
All hours	Immediate Workplace	-3.89
All hours	Any work-facility	-10.11
Entry and access through ID system		
Work related buildings		21.44
Work and other base facilities		14.11
Personal work area or office		-3.48
Access to work, base facilities, household		-32.07
Flexibility in choosing features		
Workplace Features	*All other features*	
All are off, can opt-in	all are off, can opt-in	32.04
Automatically on	all are off, can opt-in	9.11
Automatically on	all are on, can opt-out	-6.21
Automatically on	all are on, cannot opt out	-34.94
Form of the ID system		
Card or keychain to be carried at all times		29.13
Within bracelet or necklace to be worn at all times		-1.69
Within a mobile phone or PDA carried at all times		2.35
Sewn into uniforms		-3.99
Within a bracelet--alarm sounds if removed		-22.11
Ability for others find you through your ID		
Public Places	*Household*	
Automatically off, can opt-in	Automatically off, can opt-in	38.17
Automatically on, but only for emergency services	Automatically off, can opt-in	25.98
Automatically on, cannot opt-out	Automatically on, can opt out	-30.65
Automatically on, cannot opt-out	Automatically on, cannot opt-out	-33.50
Use as a payment system		
Pay on the Base	*Other forms of payment accepted*	
Yes	Yes	36.81
Yes	No	7.73
No	Yes	-37.91

A **second** key result rises from Table 4: flexibility in choosing features and the form of the ID system were important to subjects. For instance, there are big differences in subjects' preferences over a system that has opt in/out features versus a system where there is no opt out option. Similarly, subjects showed a strong aversion to a system based on non-removable ID bracelets, and a strong preference for a card/keychain-based ID tag. In both cases, the ability to remove the tag or opt out gives the subject some control over the times at which they are tracked/monitored. The implication for DoD policy makers is once again that the way an ID tagging system is "packaged" for contractors is likely to have important implications for how much contractors resist ID tagging schemes on privacy grounds. Giving people some control over ID tagging significantly increases their preference for ID tagging.

Of course, one drawback of a survey of this type is that it traces espoused preferences rather than revealed preferences, and research on privacy-related behavior does give us reason to believe that there might be differences between the two (Acquisti and Grossklags, 2005). So, like all survey results, these ones must be interpreted with suitable qualifications. On the positive side, the survey helps us better understand privacy preferences and some of the trade-offs individuals are willing to make by allowing us to measure espoused preferences using utility scores, which helps us understand the relative weight subjects put on different features of an ID tag. With this information in hand, DoD policy makers are in a better position to make informed decisions regarding the best way of introducing ID tagging as a tool for monitoring contractors. To reiterate my earlier statement: RFID tagging will only generate information if contractors wear the tags; so if DoD ever intend to use RFID tagging to monitor contractors, the system must be introduced in a way that is tolerable to the individuals who will be monitored.

CONCLUSION

To conclude this paper, I want to very briefly outline, first, research challenges that lay ahead and, second, some practical managerial issues that I see as relevant.

By future research needs, I mean research that addresses the question of "What do we need to find out about RFID?" in order that we can make better decisions about how we deploy the technology. One key question that needs researching is "How much does contractor behavior actually change when RFID monitoring is introduced?". To answer this question requires a study design that looks at behavior pre/post RFID monitoring, or contrasts two similar sites, one that has implementing RFID monitoring and one without.

Modeling might also help here. In the economic literature, monitoring is traditionally been modeled as a conflict between agents and principals, where information asymmetries are essential for agents to eek out some room for private maneuver and gain, and principles try to either close information gaps through monitoring or to align incentives in such a way that agents will behave in the interests of principles. All these issues are present in RFID monitoring, however they are also overlaid by another set of issues: security and privacy. In order to increase their private security, agents may willingly wear tags, but in order to preserve their privacy they seek commitments that safeguards are being followed regarding the collection and dissemination of information about them. Thus, modified principal-agent models that address the space that exists for deals to be made that suit both principals and agents might be helpful here.

A third researchable issue is the question of "How much RFID is enough?" In order to monitor contracts effectively, one does not need to monitor everything. This raises two points. First, sampling using RFID might be enough. For instance, CHEP (a supplier of pallets in logistics operations) does not have to tag all its pallets in order to gather population level data: it can just tag a sample of them, and generalize the data collected to the population. Second, there is the question of

precisely what data is collected. The key idea here is “thin-slicing”, i.e. the notion that just a thin slice of the overall data is enough to monitor / predict the behavior of the population. So, it may only be necessary to electronically monitor a few critical attributes of contractor performance in order for a monitoring system to add significant value.

For practicing DoD managers / policy makers, it seems to me that two key questions are fundamental to any decisions regarding RFID contractor monitoring. The first is the relative cost of using RFID. This will depend on the evolutionary path taken by the technology as well as that taken by other technologies, or alternative methods for achieving the same ends. Much may also depend on innovations in complementary technologies, such as cheap software and hardware for gathering, storing and analyzing huge quantities of RFID-generated data. Tag and reader costs are falling dramatically, and there are good reasons for thinking that these costs will continue to fall. At some point, it’s at least plausible to suggest that RFID will begin to “disrupt” other monitoring technologies, though probably in ways that seem “inferior” to present ways of doing things.

Finally, there is the question of how the law will evolve on privacy-related issues, as well as bargaining between DoD and its contractors. The shape in which RFID monitoring eventually emerges will depend on how the institutional framework comprising the law and associated institutional elements evolves. A recent GAO report (Wilshusen, 2005) has highlighted the legal ambiguities surrounding privacy and RFID, concluding that legal uncertainty was one reason why many government departments – both at the federal and state level – were not pushing forward with RFID-enabled projects, such as “chipped” driver’s licenses, “tagged” files, etc. Departments are “biding their time” until a more definitive framework of legal rules emerges. This is a good example of how “soft” institutional elements can significantly influence the pattern of evolution of innovations like RFID. Like everyone else, DoD practitioners will need to wait, anticipate, and take actions to shape the legal framework before RFID contractor monitoring can become any kind of reality.

List of References

Acquisti, A. and Grossklags, J., 2005. “Privacy and Rationality in Individual Decision Making.” IEEE Security & Privacy, January/February 2005: 24-30.

Albretch, K. and McIntyre, L., 2005. Spychips. Nashville, TN: Nelson Current.

Alchian, A and Demsetz, H. 1972. Production, Information Costs, and Economic Organization. American Economic Review 62: 777-795.

Apte, U., Dew, N. and Ferrer, G., 2006. What is the right RFID for your process? Working paper NPS-LM-06-009, Naval Postgraduate School, Monterey, CA.

Balkovich, E., Bikson, T.K. and Bitko, G., 2005. 9 to 5: do you know if your boss knows where you are? Case studies of radio frequency identification in the workplace. RAND technical report. Santa Monica, CA: RAND Corporation.

Camp, L.J. and S. Lewis, eds., 2004. The Economics of Information Security. Berlin: Kluwer.

Christensen, C.M., 2000. The Innovator’s Dilemma. Boston, MA: Harvard Business School Press.

Danneels, E., 2004. Disruptive technology reconsidered: a critique and research agenda. Journal of Product Innovation Management 21:246-258.

Dew, N., 2006. The evolution of the RFID technology system. Working paper.

Eisenhardt, K.M. (1989). Building theory from case study research. Academy of Management Review. 14(4), 532-550.

Ezzamel, M., 2004. Work organization in the Middle Kingdom, Ancient Egypt. Organization 11(4):497-537.

Foss, K. and Foss, N.J., 2005. Resources and Transaction Costs: how property rights economics furthers the resource-based view. Strategic Management Journal 26(4):541-553.

Garfinkel, S. and Rosenberg, B. 2005. RFID : Applications, Security, and Privacy. New York: Addison-Wesley.

Larson, J.S., Bradlow, E.T. and Fader, P.S., 2005. An Exploratory Look at Supermarket Shopping Paths. Working paper, Wharton business school, April 2005.

Meredith, J. (1998). Building operations management theory through case and field research. Journal of Operations Management, 16(4), 441-454.

Raynor. M., 2004. RFID and Disruptive Innovation. RFID Journal, October 2004 print edition.

Rosenberg, N. 1996. Uncertainty and Technological Change. In Fuhrer, J.C. and Sneddon Little, J., (eds.) Technology and Growth: Conference Series No.40. Boston: Federal Reserve Bank of Boston.

Singer, P.W. Corporate Warriors: the rise of the privatized military industry. Ithaca, NY: Cornell University Press

Stapleton-Grey, R., 2005. The Sorting Door: an investigation of RFID, surveillance and privacy. http://www.stapleton-gray.com/papers/DHS-poster-sgray.ppt Retrieved August 2005.

Stigler, G.J., 1980. An Introduction to Privacy in Economics and Politics," Journal of Legal Studies, 9: 623–644.

Sweeny, P.J., 2005. RFID for Dummies. New York: For Dummies.

Williamson, O.E., 1985. The economic institutions of capitalism. New York: Free Press.

Wilshusen, G.C., 2005. Information Security: Radio frequency identification technology in the Federal Government. GAO-05-551. www.gao.gov/cgi-bin/getrpt?GAO-05-551 Retrieved May 2005.

Wyld, D.C. 2005. RFID: The Right Frequency for Government. IBM Center for The Business of Government. E-Government series. Washington, DC.

Yin, R. (1994). Case study research. Beverly Hills, CA: Sage Publications.

Initial Distribution List

1. Defense Technical Information Center 2
   8725 John J. Kingman Rd., STE 0944; Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library, Code 013 2
   Naval Postgraduate School, Monterey, CA 93943-5100

3. Research Office, Code 09 1
   Naval Postgraduate School, Monterey, CA 93943-5138

4. Douglas A. Brook 1
   Dean, GB/Kb
   555 Dyer Road, Naval Postgraduate School, Monterey, CA 93943-5000

5. Keith F. Snider 1
   Associate Professor, GB/Sk
   555 Dyer Road, Naval Postgraduate School, Monterey, CA 93943-5000

6. James B. Greene 1
   Acquisition Chair, GB/Jg
   555 Dyer Road, Naval Postgraduate School, Monterey, CA 93943-5000

7. Bill Gates 1
   Associate Dean for Research, GB/Gt
   555 Dyer Road, Naval Postgraduate School, Monterey, CA 93943-5000

8. Nicholas Dew 1
   Assistant Professor, GB/Dn
   555 Dyer Road, Naval Postgraduate School, Monterey, CA 93943-5000

9. Karey L. Shaffer 1
   Program Manager, Acquisition Research Program, GB/Ks
   555 Dyer Road, Naval Postgraduate School, Monterey, CA 93943-5000

Copies of the Acquisition Sponsored Research Reports may be printed from our website www.nps.navy.mil/gsbpp/acqn/publications

THIS PAGE INTENTIONALLY LEFT BLANK

2003 - 2006 Sponsored Acquisition Research Products

Acquisition Case Series

NPS-AM-06-008 Apte, Aruna U.,and Eugene (Joe) Dutkowski. Total Ownership Cost Reduction Case Study: AEGIS Microwave Power Tubes. May 2006.

UMD-CM-05-019 Lucyshyn, William, Rene Rendon, and Stephanie Novello. Improving Readiness with a Public-Private Partnership: NAVAIR's Auxiliary Power Unit Total Logistics Support Program. July 2005.

UMD-CM-05-018 Lucyshyn, William, and Stephanie Novello. The Naval Ordnance Station Louisville: A Case Study of Privatization-in-Place. August 2005.

NPS-CM-04-008 Lucyshyn, William, Jeffrey Cuskey, and Jonathan Roberts. Privatization of the Naval Air Warfare Center, Aircraft Division, Indianapolis. July 2004.

NPS-PM-04-010 Lucyshyn, William, Keith F. Snider, and Robert Maly. The Army Seeks a World Class Logistics Modernization Program. June 2004.

NPS-CM-03-005 Lamm, David V. Contract Closeout (A). September 2003.

Sponsored Report Series

NPS-CM-06-25 Donahue, Capt Kimberly A., Capt Joshua M. Parsons. Government Imposed Constraints and Forecasting Analysis of the M.J. Soffe Corporation. December 2004.

NPS-LM-06-024 Lask, LCDR Gregory R. Advanced SEAL Delivery System: An Analysis of Product Support. July 2006.

NPS-AM-06-021 Uchytil, Capt Joseph S. Assessing the Operational Value of Situational Awareness for AEGIS and Ship Self Defense System (SSDS) Platforms through the Application of the Knowledge Value Added (KVA) Methodology. July 2006.

NPS-AM-06-020 Buchanan, Cap Steven M., Capt Jayson W. Cabell, Capt Daniel C. McCrary. Acquiring Combat Capability through Innovative Uses of Public Private Partnerships. June 2006.

NPS-FM-06-019 Jankowski, LCDR Patrick, LT Matthew Lehmann, and LT Michael P. McGee. Financing the DOD Acquisition Budget: Innovative Uses of Public-Private Partnerships. June 2006.

NPS-PM-06-018 Barnum, Usher L., Jr. Business Process Re-Engineering: Application for Littoral Combat Ship Mission Module Acquisition. June 2006.

NPS-AM-06-017 Mun, Johnathan, and Thomas Housel. A Primer on Return On Investment and Real Options Analysis for Portfolio Optimization. July 2006.

NPS-AM-06-014 Hatch II, William D. CDR, USN, Charles Gowen, AmerInd/FC Business Systems, and James Loadwick, AmerInd/FC Business Systems. Litoral Combat Ship (LCS) Civilian Aviation Alternative Support Study: Report of Findings and Recommendation. July 2006.

NPS-AM-06-012 Meyer, Jacqueline M. and Sefa Demirel. A Comparative Analysis of the Department of Defense (DoD) Passive Radio Frequency Identification (RFID) Policy and Perspective in Terms of Site Implementations. June 2006

NPS-AM-06-010 Rendon, Rene G. Using a Modular Open Systems Approach in Defense Acquisitions: Implications for the Contracting Process. January 2006.

NPS-LM-06-009 Apte, Uday M., Nicholas Dew and Gerald Ferrer. What is the Right RFID for your Process? January 2006.

NPS-LM-06-007 Mullins, Captain Michael, US Marine Corps, Captain Troy Adams, US Marine Corps and Lieutenant Robert Simms, US Navy. Analysis of Light Armored Vehicle Depot Level Maintenance. December 2005.

NPS-CM-06-006 Cortese, Captain Casey A., US Air Force, First Lieutenant Heather Shelby, US Air Force and Captain Timothy J. Strobel, US Air Force. Defining Success: The Air Force Information Technology Commodity Council. December 2005.

NPS-LM-06-005 Hernandez, Captain Emeterio V., US Air Force and Lieutenant Christopher A. Thomas, US Navy. Investigating the Department of Defense's Implementation of Passive Radio Frequency Identification (RFID). December 2005.

NPS-FM-06-004 Rios, Jr., LCDR Cesar G., US Navy. Return on Investment Analysis of Information Warfare Systems. September 2005.

NPS-AM-06-003 Komoroski, Christine L. Reducing Cycle Time and Increasing Value through the Application of Knowledge Value Added Methodology to the U.S. Navy Shipyard Planning Process. December 2005.

UMD-AM-05-021 Gansler, Jacques S., and William Lucyshyn. A Strategy for Defense Acquisition Research. August 2005.

UMD-CM-05-020 Dunn, Richard. Contractors in the 21st Century "Combat Zone." April 2005.

NPS-PM-05-017 Brianas, Christopher G. Department of the Navy Procurement Metrics Evaluation. June 2005.

NPS-LM-05-016 Doerr, Kenneth H., RADM Donald R. Eaton and Ira A. Lewis. Impact of Diffusion and Variability on Vendor Performance Evaluation. October 2005.

NPS-CM-05-015 Johnson, Ellsworth K. III, Bryan H. Paton, Edward W. Threat, and Lisa A. Haptonstall. Joint Contingency Contracting. June 2005.

NPS-CM-05-013 Schwartz, Brett M., Jadon Lincoln, Jose L. Sanchez, and Leslie S. Beltz. Update of the Navy Contract Writing Guide Phase III. June 2005.

NPS-PM-05-012 Jenkins, Glenn E., and William J. Snodgrass, Jr. The Raven Small Unmanned Aerial Vehicle (SUAV): Investigating Potential Dichotomies between Doctrine and Practice. June 2005.

NPS-AM-05-011 Apte, Aruna U. Spiral Development: A Perspective. June 2005.

NPS-FM-05-009 Jones, Lawrence R., Jerry McCaffery, and Kory L. Fierstine. Budgeting for National Defense Acquisition: Assessing System Linkage and the Impact of Transformation. June 2005.

NPS-LM-05-008 Kang, Keebom, Kenneth Doerr, Michael Boudreau, and Uday Apte. A Decision Support Model for Valuing Proposed Improvements in Component Reliability. June 2005.

NPS-PM-05-007 Dillard, John T., and Mark E. Nissen. Determining the Best Loci of Knowledge, Responsibilities and Decision Rights in Major Acquisition Organizations. June 2005.

NPS-AM-05-006 San Miguel, Joseph G., John K. Shank, and Donald E. Summers. Navy Acquisition via Leasing: Policy, Politics, and Polemics with the Maritime Prepositioned Ships. April 2005.

NPS-CM-05-003 Rendon, Rene G. Commodity Sourcing Strategies: Supply Management in Action. January 2005.

NPS-CM-04-019 Lord, Roger. Contractor Past Performance Information (PPI) In Source Selection: A comparison Study of Public and Private Sector. December 2004.

NPS-PM-04-017 Matthews, David. The New Joint Capabilities Integration Development System (JCIDS) and Its Potential Impacts upon Defense Program Managers. December 2004.

NPS-LM-04-014 Apte, Aruna. Optimizing Phalanx Weapon System Lifecycle Support. October 2004.

NPS-AM-04-013 Franck, Raymond (Chip). Business Case Analysis and Contractor vs. Organic Support: A First-Principles View. September 2004.

NPS-LM-04-006 Doerr, Ken, Donald R. Eaton, and Ira Lewis. Measurement Issues in Performance Based Logistics. June 2004.

NPS-CM-04-004 Espine, Lieutenant Commander Joseph C., and Lieutenant Commander Chong Hunter. Update of the Navy Contract Writing, Phase II. June 2004.

NPS-CM-04-002 Burger, Major Kenneth A., Captain Brian . Marine Corps Contingency Contracting MCI. Revised Manual. December 2003.

NPS-CM-04-001 Dean, Captain Chad E., and Second Lieutenant Nathan P. Vosters. Update of the Navy Contract Writing, Phase I. December 2003.

NPS-CM-03-006 Tudor, Ron B. Auto-Redact Toolset for Department of Defense Contracts. September 2003.

NPS-AM-03-004 Boudreau, Michael W., and Brad R. Naegle. Reduction of Total Ownership Cost. September 2003.

NPS-AM-03-003 Dillard, John T. Centralized Control of Defense Acquisition Programs: A Comparative Review of the Framework from 1987-2003. September 2003.

NPS-CM-03-001 MBA Team. Transformation in DoD Contract Closeout. June 2003.

Working Paper Series

NPS-LM-06-013 Dew, Nicholas. Cookies for the Real World: Assessing the Potential of RFID for Contractor Monitoring. July 2006.

NPS-PM-06-002 Dillard, John T. When Should You Terminate Your Own Program? November 2005.

NPS-AM-06-001 Naegle, Brad. Developing Software Requirements Supporting Open Architecture Performance Goals in Critical DoD System-of-Systems. November 2005.

NPS-AM-05-010 Zolin, Roxanne V., and John T. Dillard. From Market to Clan: How Organizational Control Affects Trust in Defense Acquisition. June 2005.

NPS-AM-05-005 Boudreau, Michael. Cost as an Independent Variable (CAIV): Front-End Approaches to Achieve Reduction in Total Ownership Cost. June 2005.

NPS-AM-05-002 Yoder, Elliott Cory. The Yoder Three-Tier Model for Optimizing Contingency Contracting Planning and Execution. December 2004.

NPS-AM-05-001 Yoder, Elliott Cory. Engagement versus Disengagement: How Structural & Commercially-Based Regulatory Changes have Increased Government Risks in Federal Acquisitions. November 2004.

NPS-CM-04-016 Stevens, Brett. An Analysis of Industry's Perspective on the Recent Changes to Circular A-76. October 2004.

NPS-CM-04-012 Rairigh, Beth. Air Force Commodity Councils: Leveraging the Power of Procurement. September 2004.

NPS-CM-04-011 Engelbeck, R. Marshall. Using Metrics to Manage Contractor Performance. September 2004.

NPS-LM-04-009 Eaton, Donald R. Improving the Management of Reliability. August 2004.

NPS-AM-04-007 Naegle, Brad R. The Impact of Software Support on System Total Ownership Cost. July 2004.

NPS-LM-04-003 Eaton, Donald R. Enablers to Ensure a Successful Force Centric Logistics Enterprise. April 2004.

NPS-CM-03-002 Parker, Christopher and Michael Busansky. Transformation in DoD Contract Closeout. June 2003.

Acquisition Symposium Proceedings

NPS-AM-06-011 Acquisition Research: Creating Synergy for Informed Change. April 2006.

NPS-AM-05-004 Acquisition Research: The Foundation for Innovation. May 2005.

NPS-AM-04-005 Charting a Course for Change: Acquisition Theory and Practice for a Transforming Defense. May 2004.

Technical Reports

NPS-GSBPP-03-003 Dillard, John T. Centralized Control of Defense Acquisition Programs: A Comparative Review of the Framework from 1987-2003. September 2003.

NPS-GSBPP-03-004 Boudreau, Michael W., and Brad R. Naegle. Reduction of Total Ownership Cost. September 2003.

Presentations, Publications and External Forums

Rendon, Rene. "Commodity Sourcing Strategies: Supply Management in Action." Published as "Commodity Sourcing Strategies: Processes, Best Practices, and Defense Initiatives." *Journal of Contract Management* 3, no.1 (2005): 7-21.

Doerr, Ken, Ira Lewis, and Donald Eaton. "Measurement issues in Performance Based Logistics." *Journal of Public Procurement* 5, no. 2 (2005): 164-186.

Eaton, Donald, Ken Doerr, and Ira Lewis. "Performance Based Logistics: A Warfighting Focus." *US Naval Institute Proceedings.* (In Press).

Doerr, Ken, Donal Eaton, and Ira Lewis. "Performance Based Logistics." Presented to the International Defense Acquisition Resource Management Conference. Capellen, Luxembourg, 2004.

Kang, Keebom, and Ken Doerr. Workshop: Metrics and Performance Evaluation in Performance Based Logistics. Presented at Future Naval Plans & Requirements Conference. San Diego, CA. October 2005.

Boudreau, Michael, and Brad Naegle. "Total Ownership Cost Considerations in Key Performance Parameters and Beyond." *Defense Acquisition Research Journal* 38, no.2 (2005): 108-121.

Boudreau, Michael, and Brad Naegle. Workshop: Setting up Acquisition for Total Lifecycle Supportability Performance. Presented at the Institute for Defense and Government Advancement Conference: Total Lifecycle Systems Management. Arlington, VA. 2005.

Kang, Keebom, Ken Doerr, Uday Apte, and Michael Boudreau. “Decision Support Models for Valuing Improvements in Component Reliability and Maintenance.” Submitted to the Journal of Defense Modeling and Simulation in July 2005 for possible publication. Currently the article is being reviewed by referees.

Franck, Raymond (Chip). “Business Case Analysis and Contractor vs. Organic Support: A First–Principles View.” Presented at the Western Economic Association International Annual Conference. San Francisco, CA. 5 July 2005.

Dillard, John, and Mark Nissen. “Computational Modeling of Project Organizations under Stress.” In review.

Dillard, John. “Centralization of Defense Acquisition Programs.” Accepted for publication in the Defense Acquisition Research Journal (2005).

Nissen, Mark E., and John Dillard. “Computational Design of Public Organizations.” In review.

IS4710 - Qualitative Methods. This research-seminar course has integrated the results of the FY05 Dillard-Nissen research into the students' course project.

Dillard, John T. "Centralized Control of Defense Acquisition Programs." IAMOT 2004 - New Directions in Technology Management: Changing Collaboration between Government, Industry and University. 3 -7 April 2004.

Dillard, John T. "Centralized Control of Defense Acquisition Programs: A Comparative Review of the Framework from 1987-2003." BPP Research Colloquium. 25 November 2003.

Copies of the Acquisition Sponsored Research Reports may be printed from our website www.nps.navy.mil/gsbpp/acqn/publications

THIS PAGE INTENTIONALLY LEFT BLANK

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF BUSINESS & PUBLIC POLICY
NAVAL POSTGRADUATE SCHOOL
555 DYER ROAD, INGERSOLL HALL
MONTEREY, CALIFORNIA 93943

www.nps.navy.mil/gsbpp/acqn