Information Operations Across Infospheres

Prof. Bhavani Thuraisingham* (PI)
Prof. Ravi Sandhu+ (PI)
Prof. Latifur Khan* (Co-PI)
Prof. Douglas Harris* (Consultant)

*** The University of Texas at Dallas**
+ George Mason University

Response to Air Force Office of Scientific Research BAA 2005-I

PRINCIPAL INVESTIGATOR

Dr. Bhavani Thuraisingham
Professor of Computer Science
and Director of the Cyber Security Research Center
Erik Jonsson School of Engineering and Computer Science
Box 830688, EC 31
University of Texas at Dallas, Richardson, TX 75083-0688
Tel: 972-883-4738
Fax: 972-883-2349
Email: bhavani.thuraisingham@utdallas.edu

UNIVERSITY'S ADMINISTRATION

Leslie Harper
Office of Sponsored Project
2601 North Floyd Road, MP3.218, Richardson, TX 75080
MP 3.218
Phone: 972-883-2314
Fax: 972-883-2310
E-mail: leslie.harper@utdallas.edu

EXECUTIVE SUMMARY

There is a critical need for organizations to share data within and across infospheres and form coalitions so that analysts could examine the data, mine the data, and make effective decisions. Each organization could share information within its infosphere. An infosphere may consist of the data, applications and services that are needed for its operation. Organizations may share data with one another across what is called a global infosphere that spans multiple infospheres. It is critical that the war fighters get timely information. Furthermore, secure data and information sharing is an important requirement. The challenge is for data processing techniques to meet timing constraints and at the same time ensure that security is maintained.

This proposal addresses information operations across infospheres. We first describe secure timely data sharing across infospheres and then focus on Role-based access control and Usage control in such an environment. Our goal is to send timely information to the war fighter while maintaining security. We will also address the application of game theory as well as decision centric data mining techniques to extract information from both trustworthy and untrustworthy partners of the coalition.

In particular, the **objectives** of this project are as follows:

- Develop a Framework for Secure and Timely Data Sharing across Infospheres.
- Investigate Access Control and Usage Control policies for Secure Data Sharing.
- Develop innovative techniques for extracting information from trustworthy and untrustworthy partners.

Technical Merit: While there has been work on data sharing across coalitions, an in-depth investigation of security issues as well as a study of the tradeoffs between security and timely processing has yet to be carried out. To our knowledge, this project is the first to investigate sophisticated security techniques such as Usage Control as well as decision centric data mining techniques for timely and secure data sharing across coalitions.

Broader Impact: The research to be carried out on this project is directly applicable to Network Centric Operations (NCO) that implement Network Centric Warfare (NCW). NCW promotes information sharing, shared situational awareness and knowledge of commander's intent. In addition it also enables war fighting advantage by providing synchronization, speed of command and increased combat power. We focus mainly on information sharing aspects of NCW. In particular, the results of this project can be transferred to the timely and secure data sharing services of the Network Centric Services activity being carried out by the Department of Defense.

Research Team: The research will be carried out both at the University of Texas at Dallas and at George Mason University. The principal investigators are among the leading researchers in Data and Applications Security. They have conducted innovative research in Secure Database Design, the Inference Problem, Role-based Access Control and Usage Control techniques as well as and carried out technology transfer activities. They are Fellows of IEEE, ACM, AAAS and the British Computer Society and have received prestigious awards for their research in Data and Applications Security.

INTRODUCTION

Cybercrime as well as threats to national security is costing U.S. organizations billions of dollars each year. These organizations could be government agencies, financial corporations, medical hospitals and academic institutions. There is a critical need to share data within and across organizations so that analysts could examine the data, mine the data, and make effective decisions. Each organization could share information within its infosphere. An infosphere may consist of the data, applications, and services that are needed for the operation of the organization. Organizations may share data with one another across what is called a global infosphere that spans multiple local infospheres [DEME04].

While there is an urgent need for organizations to share data across infospheres and form coalitions so that the big picture is formed especially for counter-terrorism applications and military operations as well as to gather business intelligence for marketing purposes, there is also a need to protect the information within an organization. Essentially we have a conflict between data sharing and data security. Furthermore, security also has conflicts with the timely processing of the data [THUR99]. The challenge is to enforce appropriate administration and security policies that facilitate timely data sharing as needed. Our main focus will be to examine the challenges for secure timely data sharing across infospheres operated by organizations and propose flexible architectures and techniques for accomplishing the information sharing goals. The objectives are the following:

- Develop a Framework for Secure and Timely Data Sharing Across Infospheres.
- Investigate Access Control and Usage Control Policies for Secure Data Sharing.
- Develop innovative techniques for extracting information from trustworthy and untrustworthy partners.

We propose a collaborative approach for secure timely data sharing where data, metadata, and policies are exported and integrated at the coalition level. We will develop approaches to mine the data in a collaborative peer-to-peer environment and examine the security impact. We will also develop techniques for enforcing security policies. In particular, we will focus on two of the most prominent policies: role-based policies and usage control policies invented by Ravi Sandhu ([SAND96], [PARK04]).

While much of the focus of this project will be on defensive information operations, where an organization must defend itself from attacks by remote organizations by enforcing appropriate policies, we also address situations where organizations have to operate in a hostile environment. That is, the foreign infosphere may be hostile to an organization. Now, for an organization to make effective decisions and get the big picture for many applications including detecting terrorist activities, and for combat support, it must have the necessary data. In some cases the hostile organization may not give out the critical data or it may give out false data. In such a situation, the organization must be able to utilize innovative techniques and extract information from the adversary. Essentially the organization has to carry out defensive, offensive, and intelligence information operations in order to prevent catastrophic situations. There are also some additional concerns in a hostile environment. The enemy organization may want to infiltrate our organization and find out more about our activities. In such cases, we not only have to extract information from the adversary, but we must also protect our data and activities. While this is a very challenging problem, we need to start research in this area. Therefore this project will also address applications of game theoretic and decision centric data mining techniques to extract information across the infospheres.

The research to be carried out on this project is directly applicable to Network Centric Operations (NCO) that implement Network Centric Warfare (NCW) and the notion of Communities of Interest (COI) promoted by the Department of defense. NCW promotes information sharing, shared situational awareness, and knowledge of commander’s intent. In addition it also enables war fighting advantage by providing synchronization, speed of command, and increased combat power. We focus mainly on information sharing aspects of NCW. As stated in [NCW05], one of the major challenges during Operation Iraqi Freedom (OIF) was on secure and timely information sharing. In fact General Moran states the following: “Our ability to tackle information will be drawn predominantly from US-only network, and then being able to rapidly, seamlessly move the information into a coalition network was extremely challenging. We had some work arounds that were less than fulfilling, but one of the biggest challenges we face is sharing timely information in a seamless manner with our coalition partners. That’s one of the key take aways from this conflict”.

While security has been identified as a major issue, there is little work carried out in this area. As stated in [SIGN05] by Micahel Krieger who is the director of information management in the office of the DoD deputy chief information officer, “the information assurance architecture developed last year by the National Security Agency and the COI office for the Global Information Grid (GIG) serves as the roadmap for integrating security, Krieger adds, but this will require a lot of work.” At the TechNet conference sponsored by AFCEA in May 2005, the theme was “Network Centric Operations: Balancing Speed and Agility with Security”. In fact at his keynote address General Odierno who is the Assistant to the Chairman of the Joints Chief of Staff stressed that developing security techniques and at the same time getting timely information to the war fighter is a top priority for the joint services. In addition to the activities of the DoD, the Markle report [MARK03] discusses the information sharing requirements between the different agencies including DHS, IC and DoD. The results of our research will satisfy many of the key secure information sharing requirements mentioned in the Markle report.

The organization of this proposal is as follows. The team statement will be given in Section 2. Our technical approach will be given in Section 3. In particular, first we discuss our approach to secure and timely data sharing across infospheres. Next we discuss the application of two of the more prominent and popular security policies invented by one of the authors of this proposal to a coalition environment. Finally, a discussion of the application of game theoretic and decision centric data mining techniques for information extraction will be provided. Deliverables will be discussed in section 4. The impact of the research will be listed in Section 5. Future extensions to this research will be discussed in Section 6. References, biographies of the principal investigators (PIs) and our budget for the project including cost sharing information will be appended to this proposal.

2. TEAM STATEMENT

The two main PIs for this effort are:
Prof. Bhavani Thuraisingham at the University of Texas at Dallas (UTD) and *Prof. Ravi Sandhu* at George Mason University (GMU). Prof. Thuraisingham will collaborate with *Prof. Latifur Khan* who is an expert in data mining and *Prof. Douglas Harris* who is the Executive Director of the University’s Cyber Security and Emergency Preparedness Institute and serves on the advisory board of the National White Collar Crime Center.

Dr. Thuraisingham is a leading expert in Data and Applications Security and has worked in the field for the past 20 years including 16 years at the MITRE Corporation and 3 years as IPA to the National Science Foundation establishing the Data and Applications Security program. She has designed several secure database systems including the Lock Data Views Systems at Honeywell Inc. funded by AFRL as well as Secure Object Systems and Inference Controllers at MITRE. Her work has resulted in 3 US patents, over 70 journal papers and 7 books. Her research on the unsolvability of the Inference problem was quoted by Dr. John Campbell of NSA “as the most significant breakthrough in the field in 1990” [CAMP90]. She has recently published a book on data and applications security, which has been quoted by Prof. Gene Spafford of Purdue University as “the first authoritative book in the field” [THUR05a]. She has also received the 1997 Technical Achievement award from the IEEE Computer Society and was elected a Fellow of IEEE, AAAS, and the British Computer Society. She is establishing her Consulting and Training company *BMT Security Consulting* and teaches courses at AFCEA on data management, data mining, and data security.

Prof. Ravi Sandhu is a leading expert in Information Security and is the inventor of both the widely adopted Role-based Access Control (RBAC) and Usage Control Policies (UCON). His work on RBAC is now a NIST standard. He has published extensively on access control and data security and is a Fellow of ACM and IEEE. He is also a Vice president of TriCipher, a commercial data security product development company.

Both UTD and GMU have Cyber Security Centers that have received the National Center of Excellence in Information Assurance Education by NSA and DHS. Both organizations have extensive laboratory facilities to carry out information assurance research and penetration testing. The laboratory at UTD is called SAIAL (Security Analysis and Information Assurance Laboratory) and satisfies the Tempest requirements of Mil-std-285. Researchers will be able to isolate all experiments conducted in the laboratory.

A total of 4 graduate students will be employed; 3 at UTD and 1 at GMU. Please note that UTD will provide over 100% cost share of the direct costs.

3. TECHNICAL APPROACH

Our three objectives stated in Section 1 will be carried out in Tasks I, II, and III respectively. The problem statement, background information, related work, technical issues, and our approach for Tasks I, II, and III will be elaborated in Sections 3.1, 3.2, and 3.3, respectively.

3.1 FRAMEWORK FOR SECURE TIMELY DATA SHARING ACROSS INFOSPHERES

3.1.1 Problem

Organizations including DoD, universities, hospitals, and corporations are forming coalitions to work on problems together. While data sharing is a major goal, each organization should have autonomy and control the information released to others. For various applications, especially for C4ISR, there is an urgent need to share data, extract information, and form the big picture. Furthermore it is critical that the information be sent to the war fighter in a timely manner. However, security poses restrictions to timely data sharing. The problem is to develop flexible security policies for timely data sharing and subsequently determine the amount of information that is lost by enforcing security.

3.1.2 Background

Coalition: A coalition consists of a set of organizations, which may be agencies, universities and corporations that work together in a peer-to-peer environment to solve problems such as intelligence and military operations. We assume that the members of a coalition, which are also called its partners, may be trustworthy or untrustworthy or partially trustworthy. Coalitions are usually dynamic in nature. That is, members may join and leave the coalitions in accordance with the policies and procedures. A challenge is to ensure the secure operation of a coalition.

Infospheres: Infospheres have been studied since the Air Force Scientific Advisory Board came up with the notion of Battlefield Infospheres back in the late 1990s [SAB], [MARM02]. An Infosphere is essentially the databases and services that are supported for members of an organization to carry out their operations. Infospheres are based on publish and subscribe models, consist of a number of web services and support access to heterogeneous databases and information sources. Various representations such as XML and XML schemas have been studied for data interoperability. The concept of Infospheres is also being extended to include coalition environments where there is a local infosphere for an organization and a global infosphere to support the coalition. Local and global infosphers have to interoperate securely. Figure 1 illustrates an environment where data, metadata (also referred to as a schema) and policies enforced by the local infospheres are exported to the global infosphere [HARR05], [SHET90].

3.1.3 Related Work

There has been work on coalition data sharing such as the Genoa program sponsored by DARPA [GENO], Furthermore, coalition data sharing is also discussed in an infosphere environment [MARM02]. However, security has been given very little consideration. Much of the prior work on security in a coalition environment has focused on secure federated data sharing. Thuraisingham was one of the first to propose multilevel security for federated database systems [THUR94]. Discretionary security was proposed in [MCCO95] as well as in [OLIV95]. None of the previous work has focused on determining the amount of information that is lost for conducting military operations by enforcing security. Furthermore, developing flexible policies in a coalition environment are yet to be examined. Enforcing security while meeting timing constraints remains a largely unexplored topic. For example, we have designed and developed real-time data management systems for experimental programs that support AWACS (Air Borne Warning and Control System) [BENS96]. We have also addressed information survivability issues and stressed the need for flexible policies for enforcing security and meeting timing constraints [THUR99] and some results were given in [SON95]. However, to our knowledge, no research has been reported on secure and timely data sharing for a coalition environment.

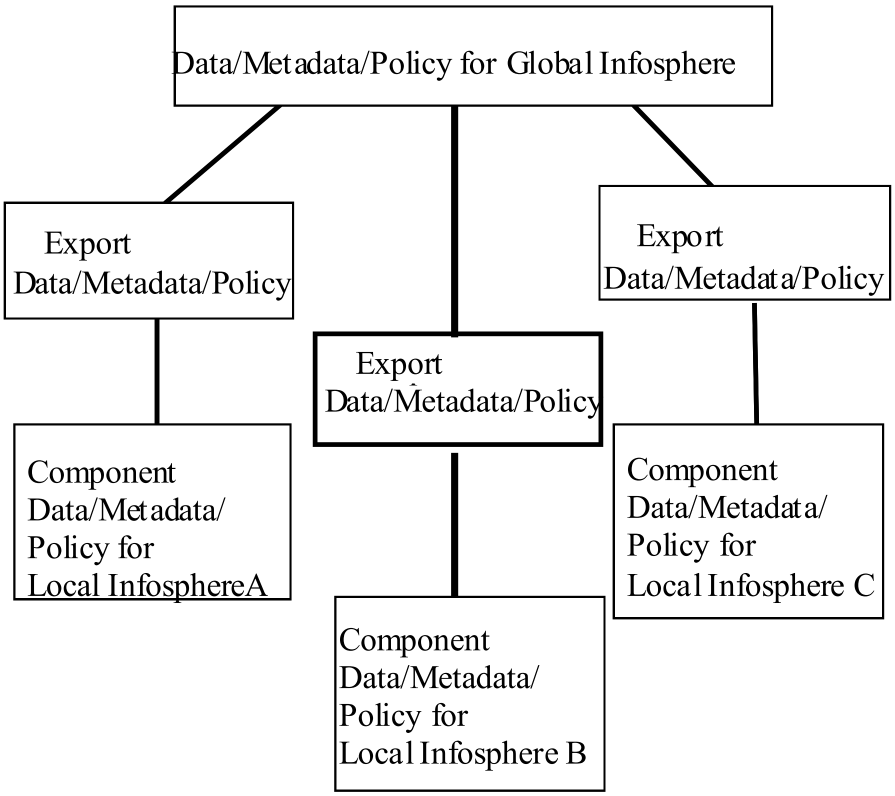
Data/Metadata/Policy for Global Infosphere
Export Data/Metadata/Policy
Export Data/Metadata/Policy
Export Data/Metadata/Policy
Component Data/Metadata/ Policy for Local InfosphereA
Component Data/Metadata/ Policy for Local Infosphere B
Component Data/Metadata/ Policy for Local Infosphere C

Figure 1. Secure Collaborative Data Management

3.1.4 Technical Issues

Data Sharing: One of the main goals of coalition data sharing is for organizations to share the data but at the same time maintain autonomy. For example, one database could be used for travel data while another database could be used to manage data pertaining to airplanes. For counter-terrorism applications and military operations, the key is to make links and associations as rapidly as possible. We need policies and procedures to determine what data to share under what conditions.

Data Mining: Data mining techniques extract patterns and trends often previously unknown from large quantities of data [THUR98]. However data mining tools could give out false positives and false negatives. This is especially critical for applications such as counter-terrorism and military operations as it could result in catastrophic consequences [THUR03]. Therefore, we need human analysts to examine the patterns and determine which ones are useful and which ones are spurious. The challenge is to develop automated tools to sift through the data and produce only the useful links and associations.

Security: Security, privacy, integrity, trust, real-time processing, fault tolerance, authorization and administration policies enforced by the component organizations via the local infospheres have to be integrated at the coalition level and enforced by the global infospehere. As illustrated in Figure 1, each organization may export security policies to the coalition. The component systems may have more stringent access control requirements for foreign organizations. The challenge is to ensure that there is no security violation at the coalition level.

3.1.4 Our Approach: Framework for Secure Timely Data Sharing Across Infospheres

* **Concept of Operation and Architecture:** First we will develop a concept of operation of the global and local infospheres. The architecture of Figure 1 will be our starting point. We will identify the interfaces between the global and local infospheres and illustrate the interactions between the different components. We will develop an example application for military operations and show how the organizations carry out secure and timely information sharing. We will utilize our experience on the TBMCS project (Theatre Battle Management System) and AWACS for developing the application as well as examine other requirements including Network Centric Operations. We will also develop scenarios to illustrate the need for secure and timely information sharing.

* **Security Policy**: Next we will develop a security policy for the coalition system. The policy will be based on a simple form of role-based access control. We will develop a policy language for specifying the policies. We will examine our previous experiences with developing policies based on XML [BERT04], RDF [CARM04] and Logic [THUR91]. The policy will include policies for the local infospheres and the global infospheres. Our focus will be on confidentiality polices and the specification will be flexible to support timing constraints. Future research will include incorporating policies for integrity and trust (please see section 6). The specification language should be generic enough to specify additional policies.

Consider the example of US, UK, Australia and Canada forming a coalition to support a combat operation. The US administrator could give access to all of his data to the US military personnel, but only give access to combat support data and the Intelligence data to the UK personnel. The administrator may restrict access only to Intelligence data to Australian and Canadian personnel. These policies will have to be specified in a unified language. Furthermore, the restrictions may be relaxed for crisis situations where all of the data by all parties may be shared if the war fighter needs the data within 30 seconds. The set of policy rules must be consistent. We also need conflict resolution rules when policies are inconsistent or not clear.

We give some examples of our work expressing policies in XML [BERT04]. In the following example we assume that Alice Brown is a General in the US Air Force working at DISA and John James is a captain at the junior level from US Army working at CECOM.

```
<General credID="9" subID = "16: CIssuer = "2">

<name> Alice Brown </name>

<country> USA <country/>

<department> AF </department>

< group> DISA </ group>

</General>

<Captain credID="12" subID = "4: CIssuer = "2">

<name> John James </name>

<country> USA <country/>

<department>Army </department>

< group> CECOM </ group>
```

```
<level> Junior </level

</Captain>
```

Next we illustrate how policies may be specified in XML. In the following example we assume the following: policies P1 and P2 state that an AF General can read all of the intelligence reports on OIF produced by the Air Force whereas he can only read the short descriptions of the report produced by the Army. Policies P5 and P6 state that a Senior Captain in the AF department can read all the asset details in the Intelligence report produced by the Air Force while he can only read certain information from assets in the Intelligence report produced by the Army.

```
<?xml version="1.0" encoding="UTF-8"?>

<policy_base>

    <policy_spec ID=‘P1' cred_expr="//General[department='CS']" target="intelligence_report.xml"
path="//OIF[@Dept='AF']//node()" priv="VIEW"/>

    <policy_spec ID=‘P2' cred_expr="//General[department='AF']" target="intelligence_report.xml"
path="//OIF[@Dept='ARMY']/Short-descr/node() and //OIF[@Dept='ARMY']/authors" priv="VIEW"/>

    <policy_spec ID=‘P3' cred_expr="//General[department='ARMY'] " target="intelligence_report.xml"
path="//OIF[@Dept='ARMY']//node()" priv="VIEW"/>

    <policy_spec ID=‘P4' cred_expr="//General[department='ARMY']" target="intelligence_report.xml"
path="//OIF[@Dept='AF']/Short-descr/node() and //OIF[@Dept='AF']/authors" priv="VIEW"/>

    <policy_spec ID=‘P5' cred_expr="//Captain[department='AF' and level='senior']" target="intelligence_report.xml"
path="//Asset[@Dept='AF']/node()" priv="VIEW "/>

    <policy_spec ID=‘P6' cred_expr="//Captain[department='AF' and level='senior']" target="intelligence_report.xml"
path="//Asset[@Dept='ARMY']/Funds/@Type and //Asset[@Dept='ARMY']/Funds/@Funding-Date" priv="VIEW "/>

    <policy_spec ID=‘P7' cred_expr="//Captain[department='ARMY' and level='junior']"
target="intelligence_report.xml" path="//Asset[@Dept='ARMY']/node()" priv="VIEW "/>

</policy_base>
```

* **Enforcement of the Policy**: We will develop algorithms for enforcing the security policies. The algorithms will include techniques for handling inconsistencies as well as resolving conflicts. Our policies will be flexible so that under certain situations (i.e. when certain triggers are activitated) only certain parts of the policies will be enforced. We will also develop techniques for exporting policies to the coalition as well as the integration of the policies at the coalition level.

We have developed inference controllers in [THUR93] and [THUR95] for database systems and we are currently developing inference and privacy controllers for the semantic web [THUR05b], [ALAM05]. We designed a primitive theorem prover for enforcing security constraints in database systems [THUR91], [THUR93]. If the policies are specified in XML or RDF or the rules language developed by W3C (world wide web consortium), then we will examine the use of Closed World Machine (CWM) as well as the Open World Machine (OWM) to enforce the security policies.

For example, CWM is a Python program that checks the properties of statements. We are currently examining modifications to CWM to handle confidentiality policies. That is, the S-CWM (which is Secure CWM) will examine the policies, reason about the policies and determine whether the policies can cause security violations. Figure 2 illustrates an architecture for policy enforcement at the Coalition level.

Information extraction and Timely information processing: We have experience using various data mining tools at MITRE and at UTD. We have also developed data mining tools in-house for web analysis and business intelligence applications [AWAD05a]. We will select a tool and use it to extract information at the coalition level and form the big picture with and without enforcing the security policies. That is, first we will extract information at the coalition level using the tools without enforcing any policies. Then we will conduct experiments enforcing variations of the policies and determine how much information is lost by enforcing security.

For example, we will first integrate the data in the coalition databases without any access control restrictions and apply the data mining tools to obtain interesting patterns and trends. In particular, we will develop associations between different data entities such as "A and B are likely to be in a location 50 miles from Baghdad". Next we will use the same tool on the integrated data after enforcing the policies. We will then determine the patterns that might be lost due to enforcing the policies. This will be an extremely useful experiment for determining the extent to which data sharing is compromised due to security.

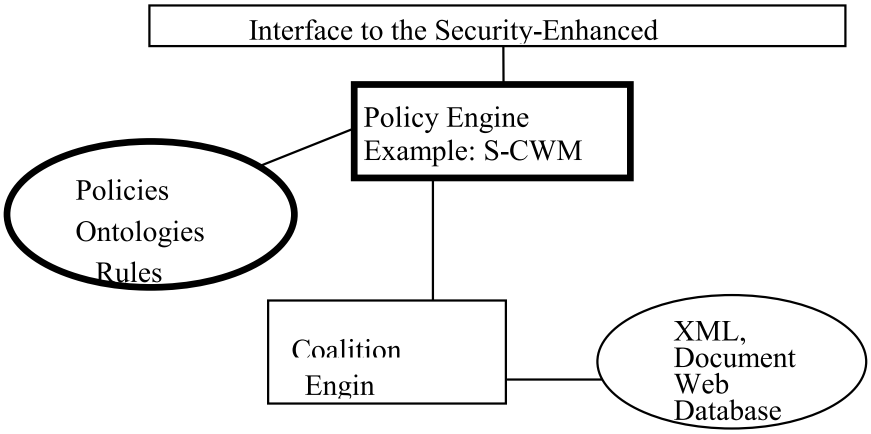

Figure 2. Enforcing Policy Enforcement Algorithms

For example, if we have a security policy rule that states the following:

"Australia cannot have any data that makes an association between A and B ",

then it may not be possible to deduce the following association rule if Australia is a member of the coalition.

"A and B are likely to be in a location 50 miles from Baghdad".

In addition, we will also conduct experiments that examine the extent to which security affects timing constraints. For example, we will enforce timing constraints on the query algorithms. That is, we will first process the query using the enforcement algorithms developed under the policy enforcement task without enforcing any of the policies. Then we will enforce the security policies and determine whether the timing constraints can be met. This will determine the extent to which security impacts timely information processing.

3.2 ROLE-BASED ACCESS CONTROL AND USAGE CONTROL POLICIES FOR INFOSPHERES

3.2.1 The Problem

In Task 1 we will apply the basic role-based access control policy for secure and timely data sharing and conduct experiments to determine the amount of information that is lost due to enforcing security. While the access control policies utilized in Task 1 is a useful and flexible policy, the security community is moving towards a full-scale role-based access control model and more recently the usage control model. However none of these models have been examined for a coalition environment. The problem is to take advantage of the features offered by both RBAC and UCON and develop security models for the global infospheres.

3.2.2 Background

RBAC: The seminal proposal on role-based access control by Sandhu et al [SAND96] introduced a general family of RBAC models called RBAC96. Subsequent work by Sandhu and his team, as well as other researchers in the community, established that RBAC is capable of expressing a wide range of policies of strong practical interest by using simple concepts. It has been demonstrated how to do conventional discretionary and mandatory access controls using RBAC, so RBAC truly encompasses previous access control models. Due to strong commercial interest by vendors and users of RBAC, the model evolved into a NIST/ANSI standard model first introduced in 2001 [FERR01] and formally adopted as an ANSI standard in 2004. The principal idea in RBAC is that users and permissions are assigned to roles, thereby users acquire permissions indirectly via roles (Figure 3).

UCON: The concept of Usage Control (UCON) was recently introduced in the literature by Park and Sandhu [PARK04]. In recent years there have been several attempts to extend access control models beyond the basic access matrix model of Lampson, which has dominated this arena for over three decades. UCON unifies various extensions proposed in the literature in context of specific applications such as Trust Management and Digital Rights Management. The UCON model provides a comprehensive framework for next generation access control. A UCON system consists of six components: subjects and their attributes, objects and their attributes, rights, authorizations, obligations, and conditions. The authorizations, obligations and conditions are the components of the usage control decisions. Another aspect that UCON extends traditional access control models is the concepts of continuity and mutability (Figure 4).

3.2.3 Related Work

Since RBAC was introduced by Sandhu and his colleagues several researchers have adapted this model for various applications. For example, Bertino et al [BERT05] have developed a temporal authorization model based on RBAC. Osborne et al [OSBO04] have developed a model for XML documents based on RBAC. Thuraisingham has examined security for the semantic web based on an RBAC-like model [THUR05c]. Applying RBAC for a coalition environment is yet to be carried out.

In the case of UCON model, Sandhu and his students have done pioneering work [PARK04]. For the first time there is now a model that encompasses all the other models. Sandhu et al have also extended UCON to handle temporal primitives. The development of UCON is still in the early stages and its application to a coalition environment has yet to be carried out.

3.2.4 Technical Issues

RBAC: RBAC is especially relevant to the protection of information in a local infosphere as well as in a global infosphere across a coalition. Administration of roles and cross-organizational roles, which are central to deployment of RBAC in infospheres are not addressed in the NIST/ANSI standard. Traditional approaches to RBAC administration often are heavyweight involving explicit actions by human administrators. These traditional approaches where a human is in the loop in every administrative decision are not scalable to the flexible and automated environment of an infosphere. Recently Sandhu and his students have introduced lightweight administration models for RBAC based on user attributes [ALKA02] and have also examined interaction of roles and workflow [KAND02]. One needs to develop administrative models for RBAC in infospheres with the goal of being as lightweight and seamless as possible without compromising security.

UCON: The new expressive power brought in by UCON is very germane to the automated and seamless security administration required in infospheres. For example, an authorization rule permits or denies access of a subject to an object with a specific right based on the subject and/or object attributes, such as role name, security classification or clearance, credit amount, etc. There may be different meanings attached to the authorization rules enforced by different local infospheres. These differences have to be reconciled. UCON is an attribute-based model, in which permission is authorized depending on the values of subject and object attributes. In a global infosphere, the challenge is to export policies that depend on the attribute values and the roles. UCON model also consists of obligations and conditions. For example, playing a licensed video file by organization A requires a user to click a notice and register in the organization's web page. Such an action can be required before or during the playing process. Mutability in

UCON means that a subject or object attribute value may be updated to a new value as a result of the access. The impact of these features in a global infosphere is yet to be examined.

3.2.5 Our Approach: Role Based Access Control and Usage Control for Infospheres

Secure information sharing, within and across infospheres, requires the enforcement of persistent access control, whereby access controls on information objects persist even as these objects reside on computers outside the immediate control of the information source. Persistent access control is a form of dissemination control (DCON) where the access policy to be enforced is inextricably linked with the object as it is moved from place to place in cyberspace. There are two major challenges in achieving this goal.

- How to enforce access controls on objects as they are physically resident on multiple computers, including end-user client computers?
- What kinds of policies are appropriate for these situations and how should they be specified?

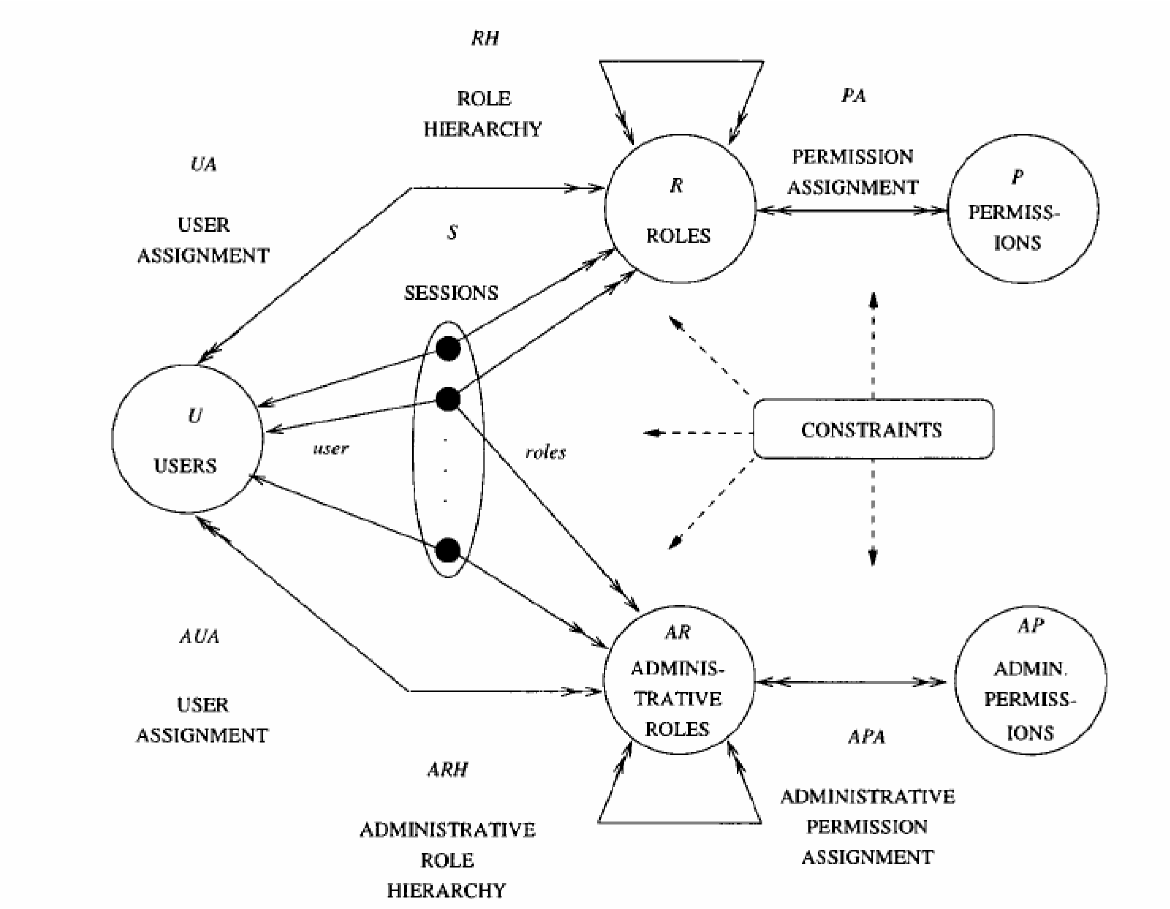

Figure 3. Role-Based Access Control (RBAC96 Model)

The first of these challenges is addressed by emerging trusted computing technologies (including the Trusted Computing Group's Trusted Platform Module, Intel's LaGrande Technology and Microsoft's Next Generation Secure Computing Base), which are anticipated to see widespread use in the near future. Recent work by Ravi Sandhu and his student Xinwen Zhang [ZHANG05] in this arena has demonstrated the enforcement of persistent access control both by ensuring that the object can be accessed only on a suitably trustworthy platform and by a suitably authorized user. Trust in the platform is established by integrity measurement and attestation protocols. Trust in the user is based on the user's identity and the user's attributes on the basis of a suitable public-key infrastructure. These technologies are expected to be widely available commercially in the next two to three years.

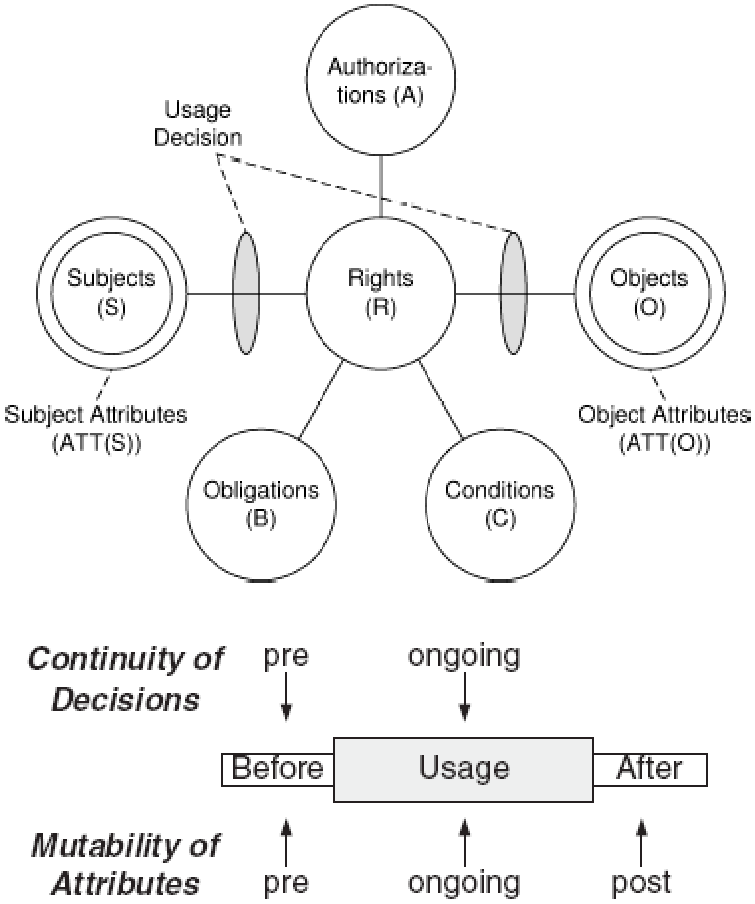

Figure 4. UCON Components

In comparison progress on the second challenge has been much slower, partly because until recently commercially viable technologies for persistent access control were not available. Given the recent push to bring these technologies to market the question of how to effectively use them to facilitate controlled information sharing in a coalition environment has become much more compelling. This second challenge is directly addressed in this project.

This project will develop a series of models for information sharing in coalitions based on Ravi Sandhu's pioneering work on role-based access control (RBAC) and usage control (UCON). The space of information sharing policies is extremely rich and varied [THOM04]. This project will partition this space in two distinct dimensions so as to build these models in a systematic manner. The first dimension distinguishes whether or not the information content in a disseminated object can be changed as the object is further re-disseminated. There are two alternatives here as follows.

- **Read-only information sharing:** In this alternative the content of an object cannot be changed as it gets disseminated. The information content remains as it was when the object was created by its source.
- **Read-write information sharing:** In this alternative the content of an object does change as it gets disseminated. There are a number of sub-cases depending on how the information can change. One possibility is to add annotations and notes to the base content which itself does not change. Another

possibility is to redact material in the process of downgrading the security level of the content. Further, the content may be modified by replacing portions of the original content with new content.

While the read-only certainly has practical applications the main purpose for treating it separately is to follow the dictum of "walk before you run." By focusing first on the read-only case it is possible to understand the issues that arise here clearly before taking on the more difficult task of dealing with writes. This incremental approach has been very productive in previous research on security models by Ravi Sandhu and seems to be the best approach for constructing models in a complex space.

The second dimension for partitioning the space of information-sharing policies is based on the scale of dissemination. In this dimension the project will study the following alternatives.

- **Small scale:** In small-scale dissemination the number of individuals who can access an object is of a small magnitude such as 10. This scale of dissemination is appropriate for the most sensitive content. At this scale it hardly seems appropriate to have very complex models. Dissemination can occur in the simple form of individual to individual (or point to point) dissemination. Some form of basic originator control where the intent of the source if the object is carried through a series of individual disseminations is the most appropriate policy. Nonetheless there are significant issues that arise. These include issues of revocation, cascading revocation, off-line access, limits on access (number of times, duration, etc.), prohibition of access (often expressed as negative rights) and transfer-only dissemination (in contrast to copy dissemination). These issues remain to be systematically addresses even in this small-scale context.

- **Medium scale:** In medium-scale dissemination the number of individuals who can access an object is of a larger magnitude such as 100's or 1000's. At this scale dissemination is best accomplished by models based on user and object attributes such as security labels, roles and other appropriate properties. The issues raised in small-scale dissemination continue to be significant here as well. In addition issues of role-to-role dissemination and delegation also arise.

- **Hybrid scale:** Hybrid scale offers a novel combination of the above two cases proposed for the first time in this project. The fundamental idea is that truly sensitive information needs to be confined to a few individuals so that actual dissemination must be small scale. Nevertheless it is impractical to achieve small-scale dissemination entirely by individual-to-individual dissemination. This is especially so in highly dynamic and mission critical applications such as the ones that the military faces. Information needs to be available to appropriate individuals when they need it. Deciding who precisely these individuals are in advance is unrealistic. Our proposal is to distinguish potential from actual dissemination. Potential dissemination is based on roles and security labels just as in the medium scale case. Actual dissemination, however, is based on the count of individuals who actually see the content. Thus a mission plan may be available to all officers of a certain rank of a coalition partner, but actual access may be limited to a small number, say, two or three. Morever during a combat situation these limits may be relaxed so actual access is available to a larger number, such as ten or fifteen. Conversely, occurrence of combat may limit the number even further to the one officer of appropriate rank who is on duty at that moment. The main goal is to enforce a small-scale of actual dissemination without pre-specifying the actual individuals who make the access, while at the same time allowing for automatic adjustments in these policies as circumstances in the real world change. The combination of RBAC and UCON is particularly powerful for expressing such hybrid policies.

Combining these two dimensions we get six combinations to investigate. This project will systematically investigate this space using a combination of RBAC and UCON to develop a series of novel models in this arena.

3.3 INFORMATION OPERATIONS ACROSS INFORSPEHERS

3.3.1 The Problem

As stated earlier, coalitions may be consist of hospitals and insurance companies, or organizations such as the United Nations, government organizations from multiple countries some possibly hostile or of universities and corporations. However, not all partners of a coalition may be trustworthy. Furthermore, the partners may not want to share data that is important for another organization. Therefore, the problem is to extract as much information as possible from one's partners without giving out much information about oneself. This problem can be divided into three sub-problems:

* How can organizations get the critical information from their partners by playing games?

* How can an organization apply decision centric data mining tools to extract as much information as possible about its partners and the information that they have?

* How can an organization find out the plans of the untrustworthy partner (i.e., an enemy capable of sabotage) without being noticed?

3.3.2 Background

Background concepts to the solutions we are proposing for the three sub-problems include game theory, data mining and offensive operations. In this section we discuss game theory and offensive operations. For a background on data mining we refer to section 3.1.2.

Game Theory: Game theory is the study of problems of conflict by abstracting the common strategies features of these problems and modeling them [JONE80]. These features are strategic and not pure chance as they are controlled by participants of the game. Two types of common games are non-cooperative and cooperative. In a non-cooperative game, no preplay communication is permitted between the players. That is, all players are for themselves. In a cooperative game, players have complete freedom of preplay communication. They may either coordinate their strategies or share payoffs.

Offensive Operations: The challenge for an organization is to find out the activities of the enemy without getting noticed. One can use the red-teaming concept to learn about the system vulnerabilities of the enemy or build honeypots [SPIT03] as well as publish advertisements to attract the enemy. For example, an advertisement to a web site may attract all kinds of users and organizations. The organization that publishes the web site will monitor the activities of various users and determine whether any of them are potential terrorists or their enemies.

3.3.3 Related Work

Game Theory Applications to Security: Various efforts on applying game theory to information security including network security have been reported [BURA]. However the most relevant effort to coalition data sharing is the game theoretic approach to building inference controllers reported in [THUR90]. To our knowledge there are no efforts on applying game theory for coalition organizations. However there are many articles in political science journals and related magazines about CIA playing games with KGB and each agency trying to thwart the other [GAME].

Decision Centric Data Mining Applications to Security: Various efforts have been reported on applying data mining for intrusion detection and auditing [AWAD04b]. A survey of these approaches is given in [THUR05d]. In addition, data mining applications in counter-terrorism is discussed in [THUR03], [THUR04]. Data mining for command and control operations was discussed in [THUR00]. None of the efforts have addressed data mining in a secure coalition environment.

Offensive Operations: Many articles have been published on carrying out offensive operations such as those appearing in AFCEA's Signal Magazine (see [SIGN05b]). For example, the May 26th2005 issue of the Washington Post states that "War game tests Web defenses: CIA running exercise to simulate large-scale cyber-assault on U.S." However only a few research articles have appeared in the Unclassified published literature. There has been work on building honeypots to attract friends as well as enemies [SPIT023]. Applications in a coalition environment have received little attention.

3.3.4 Technical Issues

Application of Game Theory: Here we assume that while the various DoD organizations share some information, the organizations do not share all of the information necessary to carry out the operation. While negotiation rules and access control rules are enforced, an organization may need more information to carry out some critical operations. In this case, organizations are the players of a game. They may play cooperative or non cooperative games depending on the relationships between them. The challenge is to determine the correct game to play for a particular scenario and develop appropriate payoff/utility functions. Bargaining with each other is also a challenge.

Decision Centric Data Mining Applications: We need to use decision centric data mining tools to extract as much information as possible about our partners and about the information that they have. The challenges include carrying out knowledge directed data mining so that false positives and false negatives may be reduced or possibly eliminated. Various feature selection techniques as well as prediction models need to be developed to determine suspicious behavior.

Offensive Operations: Offensive operations are carried out when the opposition is an enemy who is capable of sabotaging our activities. Here we need to find out what the enemy's capabilities are. While we can use data mining techniques to extract the nuggets about the enemy from the information that we have obtained about him, this may not be sufficient. We may need to find out what data they are storing and what strategies they have planned. We will need access to their databases. Essentially we need to use novel techniques such as those in game theory and determine ways to pose as legitimate users of the enemy databases and retrieve data that can save us from catastrophic events. While these types of operations are the hardest and most dangerous, we need to begin an initial investigation of such operations.

3.3.5 Our Approach: Information Operations Across Infospheres

I. Game Theory Application

Modeling query processing: To handle secure data sharing especially with untrustworthy partners, we believe that modeling the query processing scenario as a noncooperative game is more appropriate especially between two partners. The players are the partners, which could be agencies or countries of a coalition. Lets assume we have Agency A and B as two partners. The objective of agency A is to extract as much information as possible from agency B. Essentially agency A wants to compromise information managed by Agency B. B's goal is to prevent this from occurring. Cooperative games on the other hand may have applications among friendly partners of a coalition. A mixture of cooperative and non-cooperative strategies may be applied for multi-party coalition.

Two-party information sharing: We will initially model information sharing between two agencies A and B as a non-cooperative game. A has a specific objective; for example, he may know that B has some sensitive data and he wants to extract the value of that data from B. B knows A's objective. A move made by A is a query. A move made by B is the response. The game continues until A achieves his objectives or gets tired of playing the game. As stated in [JONES80], the game can be represented as a graph theoretic tree of vertices and edges. The tree has a distinguished vertex, which is the initial state. There is a payoff function, which assigns a pair of values say (X,Y) where X is the payoff for A and Y is the pay for B for each move. The payoff for A is high if he is close to obtaining the sensitive value. The payoff for B is high if the response does not reveal anything about the sensitive value. Note that if B does not give out any information or if it gives erroneous information then it cannot be regarded as a game, That is, the aim here is for B to participate in the game without giving away sensitive information.

One type of non-cooperative game that appears to work an infosphere environment is Ehrenfeucht-Fraisse Game. Such a game has been applied for mathematical logic [EHRE57] and more recently to classify database queries [CHAN82] as well as to database security [THUR90]. The Ehrenfeucht-Fraisse Game is between two non-cooperating players. The first player attempts to discern two structures such as models of databases or languages and the second player attempts to prevent the first player from doing this. In the applications of mathematical logic, the structures are models of certain formalized theories. The objective of the first player is to find a formula which is true in one model and false in the other. In the application to classify queries the structures are databases and the formula is a query, the objective of the first player is to show that there is a query which produces different results when evaluated against the two databases. For our application, the structures are:

(i) **the data that is available to agency A from agency B and**

(ii) **the data that agency B really has.**

Objective of A: If the agency A can discern between the two structures then it knows that agency B has something sensitive and can pose queries to get that information.

Objective of agency B: Act as an inference controller and prevent agency A from discerning the two structures.

We will utilize the techniques we have employed in [THUR90] for database inference control using game theory where the players are the user and the inference controller and apply them for two-party coalition data sharing. We will develop a model of the query processing strategy as well as use an appropriate payoff function that depends on the importance of the data to be extracted, the value of the data, and what A can do with the data.

Non-cooperative games have been grouped into strategic games and extensive games. Strategic games assume that the players do not have any information about the moves of the other players before they are made and extensive games assume that a player has some knowledge of the moves of others before they are made. The objective is for each player to maximize his utility and if necessary enter into a bargaining situation. Several examples and applications have been given in [OSBO94]. We will investigate these applications for the infosphere environment.

Multi-party information sharing: We will apply game theory to multi-party information sharing. The idea here is that certain parties play cooperative games while certain other parties play non-cooperative games. We will illustrate with an example consisting of three parties. As shown in Figure 5, A and C play cooperative games with common payoffs while B is an adversary. A and C play non-cooperative games with B and try to extract some sensitive values from B.

Let's consider an example. Suppose the year is 2006 and the UK has obtained some sensitive information on OIF that the US needs. However, the UK is reluctant to share this information based on its experience in 2003 as the information it supplied to the US may not have been accurate. As a result the UK citizens got very angry. Therefore, the UK does not want to take a chance. However the US in the meantime has formed an alliance with Argentina by giving some incentive either in the form of money or weapons. When the UK hears this, it is scared thinking about the Falklands. However, in reality the US has no intention of doing anything about the Falklands but does not want the UK to know the truth. So the UK reasons as follows:

The payoff UK gets by making US happy is X

The payoff UK gets by keeping Falklands is Y

The payoff UK gets by keeping its citizens happy is P

The payoff UK gets by keeping the rest of the work happy is Q

Therefore if X+Y > P+Q then the UK will give the sensitive information about OIF to the US. Otherwise the UK will likely not share the information and perhaps risk its friendship with the US.

Note that in Figure 5, A is US, B is UK and C is Argentina. The US and Argentina carry out cooperative game playing as they know of other's plans. But they play a non-cooperative game with the UK.

Cooperative games have also been called Coalition games. In a true coalition the players are friendly and therefore share the information and determine a collective payoff. However in our environment, organizations form coalitions only to solve a particular problem. An agency that is a trustworthy party in a particular coalition may turn against its partner at a later time and divulge the information gathered during the coalition operation. Therefore, while the theory of non-cooperative games is more applicable for our problem in general, as in the above example, we will develop a combination of cooperative and non cooperative game playing techniques based on an appropriate payoff/utility function.

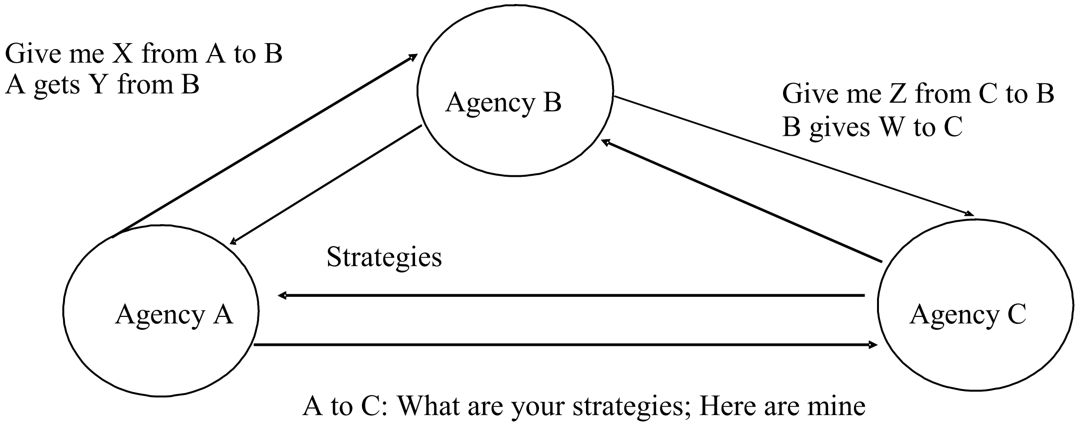

Figure 5. Multi-party Game Playing

II Decision Centric Data Mining

In a coalition environment various partners will voluntarily share some information and exchange information across various groups. We will periodically collect this information in a log file. Furthermore, this model will be extended to detect insider threats. One possibility is that hackers will gain legitimate access to a system, but then embark on a course of unauthorized use, which may include data corruption and the undermining of critical systems. In some cases sensitive information may be leaked to persons with malign intent. This kind of insider activity is now being recognized as a security threat by businesses and the government.

To mine the log file, we will take the following steps. First, we will extract features from a log file, second, we will train and test classifiers using various models, and finally, we will fuse outcomes from various models and predict the final result.

Feature Extraction: As a means of spotting abnormal activity, commands will be tracked at the operating system level. The reason for this is that monitoring at this low level permits the monitoring of all system activity whereas some activity will not be captured by application logs or command interface logs. Monitoring will also become more tightly integrated into the operating system. It will also become more difficult; both in terms of required technical skill and monitoring permission levels modifying or deleting information without leaving evidence behind. In terms of the techniques required to construct feature vectors we will carry out the following [LIU05]. The first feature representation will employ n-grams (ordered sequences of length n) of command names in a sliding window of length n over the command trace. With a shift of the window for the n-gram of 1, a given n-gram in the command trace overlaps the previous one by n-1 events. There will be an assumption of tampering and evidence of malice in an n-gram record if any of the commands making up the n-gram can be labeled malign during dataset capture [HOFM98]. The work of Liao and Vemuri [LIAO02] on external threat suggests the second feature representation. This approach uses frequency counts of command names. A statistical count of command names in a given window of W commands constitutes each record, resulting in a histogram of commands. The exact sequential information of the ordering of the commands is thrown out in this representation, except the commands of those groups within the window size W [FORR96].

Prediction Models: To predict abnormal activities, first we will train various classifiers (e.g., support vector machine [CHAN01], association rule mining, markov model and so on). Note that each classifier has its advantages and disadvantages. In WWW prediction case [AWAD05a], we observe that the Markov model is a powerful technique for predicting seen data [PITK99]; however, it cannot predict unseen data. On the other hand, SVM is a powerful technique, which can predict not only for the seen data, but also for the unseen data [CRIS00, VAPN98]. However, when dealing with too many classes or when there is a possibility that one instance may belong to many classes, SVM predictive power may decrease.

Fusion: By fusing various classifiers, namely SVM and the Markov model, we overcome major drawbacks in each technique and improve the predictive accuracy. For fusion, we use Dempster rule [LALM97, SHAF96]. Dempster's Rule is a well-known method for aggregating two different bodies of evidence in the same reference set. Suppose we want to combine evidence for a hypothesis C. Here, C is the assignment of a user activity (e.g., normal/abnormal/suspicious) during prediction for a user session. C is a member of 2^{Θ}, i.e., the power set of Θ, where Θ is our *frame of discernment*. A frame of discernment Θ is an exhaustive set of mutually exclusive elements (hypothesis, propositions). All of the elements in this power-set, including the elements of Θ, are propositions. Without loss of generality, given two independent sources of evidence m_1 and m_2, Dempster's Rule combines them in the following Equation:

$$m_{1,2}(C) = \frac{\sum_{A,B\subseteq\Theta,A\cap B=C} m_1(A)m_2(B)}{\sum_{A,B\subseteq\Theta,A\cap B\neq\phi} m_1(A)m_2(B)} \qquad (1)$$

Here *A* and *B* are supersets of C, they are not necessarily proper supersets, i.e., they may be equal to C or to the frame of discernment Θ. m_1 and m_2 are functions (also known as a *mass of belief*) that assign a coefficient between 0 and 1 to different parts of 2^{Θ}, $m_1(A)$ is the portion of belief assigned to *A* by m_1. $m_{1,2}(C)$ is the combined Dempster-Shafer probability for a hypothesis C.

Here is the pseudo-code of our approaches based on data mining technique for prediction

```
Step1. Apply Feature-Extraction
Step2.Train Classifiers
          Step2.1TrainSVM() // train SVM using one-vs-all.
          Step 2.2 Train MarkovMode
          Step 2.3 ComputeUncertainty of Various Models in Equation 1
            Step 2.3.1 ComputeUncertainty(SVM)
            Step 2.3.2 ComputeUncertainty(Markov)

Step3. For each testing session x, do
      Step 3.1. Compute $m_{SVM}(x)$ and output SVM probabilities for Different Categories.
      Step 3.2. Compute $m_{Markov}(x)$ and output Markov probabilities for Different Categories.
      Step 3.3. Compute $m_{SVM,Markov}(x)$ using Equation 1 and output the Final Prediction.
Step5. Compute Prediction Accuracy
```

III. Offensive Operations:

As we have stated, there is little work in the unclassified published literature on offensive operations. However recently we are seeing articles published in Signal magazine on the importance of monitoring the adversaries' computing activities. Our approach is to conduct a series of experiments in UTD's SAIAL laboratory on offensive operations, study the problem, and put together a plan for future research in the area.

Laboratory environment and Simulation data: SAIAL laboratory is a tamperproof laboratory where no information either in the form of data or signals can be leaked from the lab. The lab consists of mainframes, dell computers, as well as wireless test rooms. We have two sets of large data sources that we will use in our experiments. One is the Medicaid doctor/patient data set that we have obtained from the Inspector General of Texas. This is over 10 Terabytes of information, and we have Sun servers capable of processing the data. Additionally, we have the Enron email data set that we are using to conduct social network analysis to determine suspicious behavior. We will also work with COTR to obtain additional unclassified data from the Air Force.

Experiments: We will conduct the following experiments:

(i) First, we will create a coalition data sharing environment in the SAIAL laboratory using the Dell servers, and the Sun servers. We will then develop advertisements with the medical claims and insurance data for one organization. These advertisements will be monitored to analyze the behavior of the partners using the web analysis tool that we have built at UTD [AWAD05a]. (Please see section 3.3.5 Part II)

(ii) The second set of experiments is to extend the social network analysis tool that we have developed at UTD [RYAN05] and adapt it to the coalition environment. We will study the interactions between the different coalition partners and build that information into the network. Then we will use the reasoning engine associated with the social network analysis tool to determine patterns of interactions.

(iii) The third set of experiments will be carried out by the coalition administrator. The administrator will monitor the system commands typed by the coalition partners as well as the queries posed. Then we will use data mining tools and analyze the data collected by the administrator. If any behavior looks suspicious, the members of the coalition will be informed. Note that a log file will be associated with the global infosphere in Figure 1. (Please see section 3.3.5 Part II)

(iv) The fourth set of experiments is to build a honey pot, which includes fake data and attract the untrustworthy partners to the fake data. This way we can determine which of the partners of the coalition are untrustworthy. Note that this set of experiments is more of a defensive operation rather than an offensive operation.

(v) The fifth set of experiments is to build “red-team-like vulnerability” attacks. Members of the team are UTD students who are US citizens. In our Data and Applications security team, the students include Ryan Layfield, Nathalie Tsybulnik, Gal Lavee, and Joe Whittaker. We will also use industry experts with experience for guidance and advice as approved by the COTR).

Novel Techniques: Note that there have been efforts on conducting similar experiments such as the one mentioned in the Washington Post article on May 26th 2005. Furthermore, the adversary knows about the published vulnerabilities and will very likely turn off the libraries and code that can be exploited by its partners. Therefore we need to develop novel techniques. Three of the techniques that we are exploring are the following:

Trojan Image Exploitation: Modern anti-virus and anti-spy ware detection packages rely on the presence of malicious code within an executable or script to prevent attacks. This is done by detection methods that are carried out when the program first loads. In theory, it is possible to circumvent this detection by designing a program without any explicit malicious code; instead, a memory leak in this program’s security is purposefully created. This weakness is exploited by downloading a tailored file from the Internet, such as a picture, after the program is loaded. As a result, this program could be used as a staging area for a malicious attack.

Web Browser Customization: Web browsers have been enhanced dramatically in the past year to prevent attacks from malicious web pages. For the benefit of the user, these features are frequently made optional, allowing a great deal of customization. By compromising a user’s customization features covertly, it becomes possible to execute potential attacks without the user detecting any warning signs normally visible in the user’s browser such that the attacker’s methods can be hidden from the user. The attacker could use browser customization, such as enabling JavaScript, to create a shadow copy of the web and gain classified information from the victim without certain warning signs, such as URLs being correctly displayed. All user-entered information would be funneled through the attacker’s spoofed world and thus the attacker could easily take advantage of the situation in order to retrieve any type of information.

Message Interception: We will use the Enron data set and send emails to the partners of the coalition as well as to those outside of the coalition. We will simulate the messaging in such a way that they are sent at random intervals. We will then determine whether interception techniques can be used to extract some of the messages sent. This is a very challenging problem and we will carry out an initial investigation on this topic. Based on the results of the experiments, we will produce a plan for future directions on offensive operations research at the unclassified level.

Measurements: As stated earlier, the data to be used will come from an Enron e-mail dataset and a vast database of medical records (more than 10 terabytes). We will also work with the COTR to obtain Air Force data. A security policy will be written in regards to these datasets and each requirement in the policy will be tagged critical or non critical. In order to measure the accuracy of the simulations, the protector of the policy will attempt to guard each policy, especially those considered critical, whereas the attacker will make it a priority to compromise the critical policies. Thus the critical policies will be of higher value whereas non critical policies will have lesser value. In this way, the results can be quantified by measuring the success of the defense and the success of the attacks, depending on the simulations.

4. RESEARCH TASKS, DELIVERABLES AND MILESTONES

Task 1: Framework for Secure Data Sharing (UTD and GMU; Year 1 and Year 2)

We will develop a framework for secure timely data sharing and data mining. The framework will consist of the following:

* Architecture for secure timely data management which includes components for data/metadata integration and policy integration
* Language for specifying various policies including security and real-time policies
* Techniques for secure data sharing including those for enforcing the policies between organizations
* Capability for applying data mining tools on the data that is shared.
* A concept of operation of the coalition environment.

We will conduct experiments with total data sharing and partial data sharing and examine the patterns that are obtained in both cases. How much information is lost by not sharing all of the data between organizations? We will also demonstrate the impact of imposing timing constraints on the query algorithms. Prototype implementation of the framework will be developed and demonstrated.

Task 1 Deliverables: Year 1: Interim Report
Year 2: Final Report; Proof of Concept Demonstration including software and instruction manual

Task 2: Access Control (GMU; Year 1, Year 2 and Year 3)

We will investigate the use of Role-based and Usage Control policies in the collaborative environment. We will specify the policies and develop techniques to enforce the policies across infospheres. Prototypes for RBAC and UCON techniques will be demonstrated.

Task 2 Deliverables: Year 1: Interim Report
Year 2: Final Report, Proof of Concept Demonstration including software and instruction manual

Task 3: Information Operations (UTD; Year 2 and Year 3)

* Develop a framework based on game theory for organizations to play games with one another and maximize their benefits. Both cooperative and non-cooperative game theoretical techniques will be investigated. The objective is for an organization to extract as much information as possible from its partners without giving out much information about itself.
* We will apply decision centric data mining techniques to extract information about our partners and from our partners, especially on untrustworthy partners in the coalition to extract the information needed for our operations but remain sensitive to our partners.

* We will conduct a preliminary investigation of techniques for carrying out offensive operations as discussed in section 3.3.3.

Task 3 Deliverables: Year 2: Interim report on the application of game theoretic techniques, Interim report on the applications of data mining techniques, Interim report on the experiments to be carried out for offensive operations.
Year 3: Final reports on game theory applications, data mining applications, and details of offensive operations and research plan
Proof of concept demonstrations of game theory applications, data mining applications, and offensive operations. Deliverables will include software and instruction manuals

5. IMPACT OF THE RESEARCH AND OUTREACH

Technical Contributions: This research will have a tremendous impact (please see technology transfer activity below) not only on the Department of Defense and Intelligence organizations but also on organizations forming coalitions and working with partners. Recently there has been much debate on data sharing vs. security. However, little work has been reported on sharing data and at the same time maintaining security and timely information processing. This effort will provide some solutions and also determine how much useful data has been lost by incorporating security controls. Access control and Usage control models will be examined for coalition data sharing. The information operations effort will provide some guidance as to how organizations can play games with each other and extract as much information as possible from the partners who are non-cooperative. In addition, we will also provide a research plan for the problem of finding out more information about the adversary's activities.

Publications and Patents: The investigators have extensive publications records. They have patents that have been lucrative and have authored books in data security. They will publish the results as permitted by the COTR. Furthermore, the investigators will apply for patents based on the advice from Counsel and the COTR. The investigators also plan to continue writing textbooks in data and applications security topics and will include the research results in the publications as approved by the COTR.

Technology Transfer: The research will be transferred to Air Force programs as well as to the Joint services at every opportunity. The investigators have supported AFRL researchers and various Air Force programs. Dr. Thuraisingham has worked on experimental research programs for Air Force Systems while she was at MITRE including the AWACS and TBMCS systems. She has also participated in panels at the Scientific Advisory Board. The PIs will work with the COTR to identify one or two Air Force programs and transfer the technology. As permitted by the COTR we will install the software and deliver instruction manuals for the AF to experiment with our technologies. The research is also directly applicable to NCW and NCO (the implementation of NCW). We will work closely with those involved in NCO as well as COIs for the DoD and transfer the results to the programs as permitted by the COTR. We will also give presentations to major DoD contractors including Raytheon, Boeing and Lockheed corporations. Many of these corporations have large subsidiaries in the Dallas Metropolitan area and UTD, through Dean Bob Helms (Erik Jonsson School of Engineering and Computer Science), has access to high-level officials at these corporations. We will also work with corporations such as IBM, which already have security products to transfer the technology as permitted by the COTR. Prof. Sandhu is in the Washington area and will give presentations of this research to government organizations. In addition, he is the founder of TriCipher Corporation and will incorporate the results as much as possible into his product as approved by the COTR.

Teaching: The investigators are teaching various courses in data and applications security and information security. They will incorporate the results into their teaching both at the University of Texas at Dallas and at George Mason University. Prof. Thuraisingham is also an instructor at AFCEA PDC for the past 7 years and teaches courses on data management, data security and data mining. These courses are offered at AFCEA headquarters as well as at different military installations (e.g., Offutt and Eglin AFB). Prof. Thuraisingham has also given courses to various DoD organizations including NSA, ESC, SPACECOM, AIA, SPAWAR, EUCOM, DISA and CECOM. Furthermore, the PIs give numerous keynote addresses at government, research and commercial conferences (e.g, Federal Database Colloquium by AFCEA from 1994 until 2001 and SAS Data Mining Conference 1999 and 2005). The PIs as well as the Co-PIs give several tutorials at research conferences including the WWW conference and IEEE COMPSAC conference. They will use material from the research as approved by the COTR.

6. FUTURE EXTENSIONS

There are several directions for future research. We list some.

Multilevel Security: We need to examine multilevel security for coalition data sharing. We have carried out an extensive investigation of multilevel security for relational systems, object system, deductive databases, distributed databases and federated databases. The need for multilevel security for DoD coalitions in discussed in [SIGN05].

Policies for Trust, Privacy, Integrity and Data Quality: The research to be carried out on the project will focus on confidentiality and real-time processing policies for secure timely data sharing. Future work will include extensions for privacy, trust, data quality, and integrity. On May 24th IBM announced new software to provide security without sacrificing privacy (please see New York Times, May 24th). Such products and techniques have to be examined for a coalition data sharing environment.

Identity Management: In addition to security management, an investigation of identity management in a coalition environment is needed.

Attacks on Real-time processing: In our investigation we will examine the impact on enforcing access control on real-time processing. A more sinister problem is the malicious attack on the timely processing of data. Research is just beginning in this area. We need to investigate the issues for coalition data sharing.

Novel techniques: We will investigate game theory for information extraction as well as use mining techniques. There are also other techniques that we have used for inference control and these should be investigated for secure data sharing. Topics include the applications of mathematical programming, Inductive inference, and probabilistic calculus. Additional game theoretic techniques need to be explored.

Information Operations: Our investigation of offensive operations will be to conduct experiments and subsequently produce a plan for research. This research plan will specify the directions for future work.

Immune System Model: The Markle report has recommended the Immune System Model to DHS. The immune system attacks the "bad organisms" and leaves the "good organisms" alone. When it starts attacking the "good organisms" then one gets autoimmune diseases. The report suggests that techniques need to be developed for an organization to attack its enemies and not its friends. We need to examine this approach for coalition data sharing.

Social Network Analysis: We have developed a simple social network analysis tools and tested it with the Enron data set that we have obtained. In this project we will use this tool to carry out the experiments. However in a coalition environment there will be complex relationships between different organizations and cultures. Therefore we need more sophisticated tools to model these relationships and carry out analysis.

REFERENCES

[ALKAS02] Mohammad Al-Kahtani and Ravi Sandhu, "A Model for Attribute-Based User-Role Assignment." *Proc. 17th Annual Computer Security Applications Conference*, Las Vegas, Nevada, December 9-13, 2002, pages 353-362.

[ASHR05] A. Ashraful, L. Khan and B. Thuraisingham, Design and Implementation of the Privacy Controller for the Semantic Web, Technical Report, the University of Texas at Dallas, To be Submitted to Data and Knowledge Engineering Journal.

[AWAD05a] M. Awad, Latifur Khan, and Bhavani Thuraisingham, Predicting WWW Surfing Using Multiple Evidence Combination, Accepted in VLDB Journal 2005.

[AWAD05b] M. Awad, Latifur Khan, and Bhavani Thuraisingham, *A New Intrusion Detection System Using Support Vector Machines and Hierarchical Clustering,* Accepted in VLDB Journal, 2005

[BENS96] E. Bensley, B. Thuraisingham, et al, Design of a Infrastructure and Data Management for Real-time Command and Control System, Proceedings IEEE WORDS, 1996.

[BERT04] E. Bertino, B. Carminati, E. Ferrari and B. Thuraisingham, *Secure Third Party Publication of XML Documents*, IEEE Transactions on Knowledge and Data Engineering, October 2004

[BERT05] E. Bertino, J. Joshi, et al, A Generalized Temporal Role-Based Access Control Model. IEEE Trans. Knowl. Data Eng. Vol. 17, 2005

[BURA] Chiranjeeb Buragohain, Game Theory in Ad-hoc Networks, http://www.cs.ucsb.edu/~ebelding/courses/595/s04_gametheory/overview.pdf

[CAMP90] John Campbell, Database Security, Proceedings of the National Computer Systems Security Conference, Washington DC, October 1990.

[CARM04] B. Carminati, E. Ferrari, B. Thuraisingham, RDF Security, Proceedings DEXA Conference Zaragoza, Spain, August 2005.

[CHAN01] Chih-Chung Chang and Chih-Jen Lin, LIBSVM: a library for support vector machines, 2001, http://www.csie.ntu.edu.tw/~cjlin/libsvm

[CRIS00] N. Cristianini and J. Shawe-Taylor, Introduction to Support Vector Machines, Cambridge University Press 2000 ISBN: 0 521 78019 5

[DEME04] A. Demers, J. Geherke, and M. Riedewald, Research Issues in Mining and Monitoring of Intelligence Data, Next Generation Data Mining. AAAI Press, 2004 (Ed: H. Kargupta et al)

[EHFR57] Ehrenfeucht, A. Application of games to some problems of mathematical logic. Bull. Acad. Polon. Sci. Cl. III. 5, 1957.

[FERR01] David F. Ferraiolo, Ravi Sandhu, Serban Gavrila, D. Richard Kuhn and Ramaswamy Chandramouli. "Proposed NIST Standard for Role-Based Access Control." *ACM Transactions on Information and System Security*, Volume 4, Number 3, August 2001, pages 224-274.

[FORR96] S. Forrest, S. Hofmeyr, A. Somayaji, and T. Longstaff. A Sense of Self for Unix Processes. In Proceedings of 1996 IEEE Symposium on Computer Security and Privacy. 1996.

[GAME] http://www.gametheory.net/

[GENO] Tom Armor, DARPA Genoa program, DARPATECH Presentations, CA 2002.

[HARR05] D. Harris, L. Khan, B. Thuraisingham, "Standards for Secure Data Sharing across Organizations," Accepted in Computer Standards and Interfaces Journal, 2005 (subject to revision)

[HOFM98] S. Hofmeyr, S. Forrest, and A. Somayaji. Intrusion Detection Using Sequences of System Calls. InJournal of Computer Security Vol. 6, pages 151-180. 1998

[JONE80] A. Jones, Game Theory, Mathematical Models of Conflict, Halstead Press, 1980.

[KAND02] Savith Kandala and Ravi Sandhu, "Secure Role-Based Workflow Models." Database Security XV: Status and Prospects, (D. Spooner, editor), Kluwer 2002.

[LALM97] M. Lalmas. Dempster-Shafer's Theory of Evidence Applied to Structured Documents: Modeling Uncertainty. *ACM SIGIR Conference on Research and Development in Information Retrieval*, pp 110-118, Philadelphia, PA, July 1997.

[LAYF05] Ryan Layfield, L. Khan, and B.. Thuraisingham, "Social Network Analysis," Technical Report, University of Texas at Dallas, to be submitted to the Journal of Information Systems Management.

[LIAO02] Y. Liao and V. Vemuri. Using Text Categorization Techniques for Intrusion Detection. In Proc. 11th USENIX Security Symposium, pages 51-59. August 2002.

[LIU05] Alexander Liu, Cheryl Martin, Tom Hetherington, and Sara Matzner, A Comparison of System Call Feature Representations for Insider Threat Detection, Proceedings of the 2005 IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY June 2005

[MARK03] Creating a Trusted Network for Homeland Security, Markle Report, 2003 (Editor: M. Vatis)

[MARM02] Robert E. Marmelstein, Force Templates: A Blueprint for Coalition Interaction within an Infosphere, IEEE Intelligent Systems, Volume 17, 2002.

[MCCO95] Cathy Mccollum, B. Blaustein et al, Autonomy and Confidentiality: Secure Federated Data Management. Proceedings, NGITS 1995.

[NCW05] The Implementation of Network Centric Warfare, Office of Force Transformation, 2003.

[OLIV95] Martin S. Olivier: Self-protecting Objects in a Secure Federated Database, Proceedings of the IFIP Database Security Conference, NY, August 1995.

[OSBO94] M. Osborne, A. Rubinstein, A Course in Game theory, MIT Press, 1994.

[OSBO04] S. Osborn and J. Wang, A role-based approach to access control for XML databases, Proceedings SACMAT 2004.

[PARK04] Jaehong Park and Ravi Sandhu. "The $\mathrm{UCON}_{\mathrm{ABC}}$ Usage Control Model." *ACM Transactions on Information and System Security*, Volume 7, Number 1, February 2004.

[PITK99] James Pitkow and Peter Pirolli. Mining longest repeating subsequences to predict World Wide Web surfing. In *Proc. of 2nd USENIX Symposium on Internet Technologies and Systems (USITS'99).*Boulder, Colorado, October 1999.

[SAB] US Air Force Scientific Advisory Board *, Report on Building the Joint Battlespace Infosphere,* tech. report SAB-TR-99-02, US Air Force, Washington, D.C., 1999; www.sab.hq.af.mil/archives/reports/index.htm

[SAND96] Ravi Sandhu, Edward Coyne, Hal Feinstein and Charles Youman, "Role-Based Access Control Models." *IEEE Computer*, Volume 29, Number 2, February 1996.

[SHAF96] Glenn Shafer. *A Mathematical Theory of Evidence.* Princeton University Press, 1976.

[SHET90] A. Sheth and J. Larson, Federated Database Systems, ACM Computing Surveys, September 1990.

[SIGN05a] Signal Magazine, AFCEA, May 2005

[SIGN05b] Signal Magazine, AFCEA, February 2005

[SNAR] SNARE (available at http://www.intersectalliance.com/projects/Snare/index.html

[SPIT02] Lance Spitzner, Honeypots, Tracking Hackers, Addison Wesley, 2002.

[SON95] S. Son, R. David and B. Thuraisingham, *An Adaptive Policy for Improved Timeliness in Secure Database Systems,* Proceedings of the 9th IFIP Working Conference in Database Security, New York, August 1995.

[THUR90] B. Thuraisingham, *Novel Approaches to the Inference Problem*, June 1990, Proceedings of the 3rd RADC Database Security Workshop, New York.

[THUR91] B. Thuraisingham, *A Nonmonotonic Typed Multilevel Logic for Multilevel Database Management Systems*, June 1991, Proceedings of the 4th IEEE Computer Security Foundations Workshop, Franconia, NH.

[THUR93] B. Thuraisingham, W. Ford, M. Collins and J. O'Keeffe, *Design and Implementation of a Database Inference Controller*, December 1993, Data and Knowledge Engineering Journal (North Holland), Vol 11, #3

[THUR94] B. Thuraisingham, *Security Issues for Federated Database Systems,* 1994, Computers and Security (North Holland), December 1994.

[THUR95] B. Thuraisingham and W. Ford, *Security Constraint Processing in a Multilevel Secure Distributed Database Management System,* IEEE Transactions on Knowledge and Data Engineering, April 1995

[THUR98] B. Thuraisingham, Data Mining: Technologies, Techniques, Tools and Trends, CRC Press, December 1998.

[THUR99] B. Thuraisingham and J. Maurer, *Information Survivability for Real-time Command and Control Systems*, IEEE Transactions on Knowledge and Data Engineering, January 1999

[THUR00] B. Thuraisingham and M. Ceruti, Understanding and Applying Data Mining for C3I Applications, Proceedings IEEE COMPSAC, 2000.

[THUR03] B. Thuraisingham, Web Data Mining and Applications in Business Intelligence and Counter-terrorism, CRC Press, Boca Raton, FL, 2003.

[THUR04] B. Thuraisingham, *Data Mining for Counter-terrorism*, AAAI Press (in Next Generation Data Mining, Editor: H. Kargupta et al), 2004

[THUR05a] B. Thuraisingham, Database and Applications Security: Integrating Information Security and Data Management, CRC Press, May 2005

[THUR05b] B. Thuraisingham, *Privacy Constraint Processing in a Privacy-Enhanced Database Management System*, Accepted for publication in Data and Knowledge Engineering Journal (North Holland), 2005.

[THUR05c] B. Thuraisingham, Security Standards for the Semantic Web, Computer Standards and Interface Journal, March 2005.

[THUR05d] B. Thuraisingham, *Managing Cyber Threats*: Issues and Challenges, Kluwer (editor: V. Kumar et al), Kluwer, 2005.

[THOM04] Roshan Thomas and Ravi Sandhu, "Towards a Multi-Dimensional Characterization of Dissemination Control." *Proc. 5th IEEE International Workshop on Policies for Distributed Systems and Networks*, New York, June 7-9, 2004, pages 197-200.

[TSYB05] Natalie Tsybulnik, L. Khan and B. Thuraisingham, Design of an Inference Controller for the Semantic Web, Technical Report, the University of Texas at Dallas, To be submitted to the Journal of the Semantic Web.

[VAPN98] V. Vapnik. Statistical Learning Theory. Wiley, New York, 1998.

[ZHANG05] Xinwen Zhang and Ravi Sandhu, "Peer-to-Peer Access Control Architecture Using Trusted Computing Technology." Proc. 10th ACM Symposium on Access Control Models and Technologies (SACMAT), Stockholm, June 1-3, 2005.

INVESTIGATORS: The Biographies of the Team are given below.

Dr. Bhavani Thuraisingham has recently joined The University of Texas at Dallas as a Professor of Computer Science and Director of the Cyber Security Research Center in the Erik Jonsson School of Engineering. She is a Fellow of the IEEE (Institute for Electrical and Electronics Engineers) and AAAS (American Association for the Advancement of Science). She received IEEE Computer Society's prestigious 1997 Technical Achievement Award for "outstanding and innovative contributions to secure data management". She was elected a Fellow of the British Computer Society in February 2005.

Thuraisingham's research in information security and information management has resulted in over 70 journal articles, over 200 refereed conference papers, and three US patents. She is the author of seven books in data management, data mining and data security including one on data mining for counter-terrorism and another on Database and Applications Security. She has given over 25 keynote presentations at various research conferences and has also given invited talks at the White House Office of Science and Technology Policy and at the United Nations on Data Mining for counter-terrorism. She serves (or has served) on editorial boards of top research journals. Thuraisingham is also establishing the consulting company "*BMT Security Consulting* "specializing in Data and Applications Security consulting and training and is the Founding President of the company.

Prior to joining the University of Texas at Dallas, Thuraisingham was an IPA (Intergovernmental Personnel Act) at the National Science Foundation from the MITRE Corporation. At NSF, she established the Data and Applications Security Program and co-founded the Cyber Trust theme and was involved in inter-agency activities in data mining for counter-terrorism. She has been at MITRE from January 1989 until June 2005 and has worked in MITRE's Information Security Center and was later a department head in Data and Information Management as well as Chief Scientist in Data Management. She has served as an expert consultant in information security and data management to the Department of Defense, the Department of Treasury and the Intelligence Community for over 10 years and is an instructor for AFCEA (Armed Forces Communication and Electronics Association) since 1998. Thuraisingham's industry experience includes six years of product design and development of CDCNET at Control Data Corporation and research, development and technology transfer at Honeywell Inc. Her academia experience includes visiting faculty at the New Mexico Institute of Technology, Adjunct Professor of Computer Science first at the University of Minnesota and later at Boston University. Thuraisingham was educated in the United Kingdom both at the University of Bristol and at the University of Wales.

Dr. Ravi Sandhu is Professor of Information and Software Engineering and Director of the Laboratory for Information Security Technology (www.list.gmu.edu) at George Mason University. He is a leading authority on access control, authorization and authentication models and protocols. His seminal paper on role-based access control (RBAC) introduced the RBAC96 model, which evolved into the 2004 NIST/ANSI standard RBAC model (and is on track to become an ISO standard). More recently he introduced the Usage Control (UCON) model as a foundation for next-generation access control by integrating obligations and conditions with the usual notion of authorization in access control and providing for continuity of enforcement and mutability of attributes. Previously he has published influential and widely cited papers on various security topics including safety and expressive power of access control models, lattice-based access controls, and multi-level secure relational and object-oriented databases.

He is a Fellow of the ACM and a Fellow of IEEE. He has published over 160 technical papers on computer security in refereed journals, conference proceedings and books. He founded the ACM Transactions on Information and Systems Security (TISSEC) in 1997 and served as editor-in-chief until 2004. He served as Chairman of ACM's Special Interest Group on Security Audit and Control (SIGSAC) from 1995 to 2003, and founded and led the ACM Conference on Computer and Communications Security (CCS) and the ACM Symposium on Access Control Models and Technologies (SACMAT) to high reputation and prestige. Most recently he founded the IEEE Workshop on Pervasive Computing Security (PERSEC) in 2004. His research has been sponsored by numerous public and private organizations currently including Lockheed Martin, Northrop Grumman, Intel, Verizon, Network Associates, DARPA, DOD, DOE, NSA, NRO, NSF, NRL, IRS, and ARDA. He has provided high-level security consulting services to several private and government organizations. Ravi Sandhu has also served as the principal designer and security architect of TriCipher's Armored Credential System (TACS), which earned the coveted FIPS 140 level 2 rating from NIST. Ravi Sandhu earned his B.Tech. and M.Tech. degrees in Electrical Engineering from the Indian Institutes of Technology at Bombay and Delhi respectively, and his M.S. and PhD degrees in Computer Science from Rutgers University.

Dr. Latifur R. Khan has been an Assistant Professor of Computer Science department at University of Texas at Dallas since September, 2000, heads the data mining research group, and is the director of the database laboratory. He received his Ph.D. and M.S. degree in Computer Science from University of Southern California (USC) in August 2000 and December 1996 respectively. Professor Khan is currently supported by grants from the *National Science Foundation (NSF), Alcatel, USA* and has been awarded the *Sun Equipment Grant*. Dr. Khan has more than fifty articles, book chapters, and conference papers focusing in the areas of: database systems, multimedia information management, data mining applications in intrusion detection, biometrics and bioinformatics. His articles have appeared in the VLDB journal (ACM/VLDB joint publication) and the, Bioinformtics journal by Oxford University press. He currently serves on the editorial board of North Holland's Computer Standards and Interface Journal.

Professor Khan has served as a referee for database journals, conferences (e.g., IEEE TKDE, KAIS, ADL, VLDB) and he served as a program committee member for Eleventh ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (SIGKDD2005), ACM Fourteenth Conference on Information and Knowledge Management (CIKM 2005), International Conference on Database and Expert Systems Applications DEXA 2004, and International Conference on Cooperative Information Systems (CoopIS 2004). He served as program chair of ACM SIGKDD International Workshop on Multimedia Data Mining, 2004.

Dr. E. Douglas Harris is the Associate Dean of the Erik Jonsson School of Engineering and Computer Science at The University of Texas at Dallas (UTD). He is also the Executive Director of the CyberSecurity and Emergency Preparedness Institute. Under his direction UTD received the National Center of Academic Excellence in Information Assurance Education recognition from the National Security Agency (NSA) and the Department of Homeland Security (DHS).

For the past six years, Dr. Harris has been UTD's principle investigator for the worldwide telecommunications industry's Quality Measurements Repository System (MRS) for the QuEST Forum. The system was designed to meet very rigorous confidentiality, security, reliability, and availability requirements. The QuEST Forum is an international consortium of service providers and suppliers. The UTD MRS Computer Information System is considered to be one of the most secure in the world and meets the rigid British Standards Institute Standard BS 7799 for Information Security. Since the spring of 2000, Dr. Harris has been UTD's principle investigator for an EPA funded emergency response system– called "E-Plan." The system allows first responders to instantly view critical hazardous material information and emergency plans at the site during emergencies. This program has been implemented in several key regions across three states; Texas, Louisiana and Arkansas. It is currently considered one of the best first responder information programs in the U.S. to help mitigate hazmat incidents and terrorist acts.

Dr. Harris started his career at Texas Instruments where he spent over 20 years. From 1967 to 1978 he was corporate manager of automation at TI. After joining the academic ranks at Southern Methodist University (SMU) in 1978 he also served as the Vice President at Productivity International, Inc. where he completed several major consulting jobs in the area of CAD/CAM systems and Management of Technology. In 1988 he was appointed Assistant Dean in the School of Engineering and Applied Sciences (SEAS) at SMU. He has been the committee chair and dissertation advisor for twelve (12) doctoral students. He served on nineteen (19) other doctoral committees, published over 40 papers and has taught in both engineering and business schools.

BUDGET AND JUSTIFICATION

Budget requested for 3 yrs from AFOSR is $300,105
GMU portion of the budget is $150K (approx 50K/yr)
UTD portion of the budget is approx. $95K
UTD will cost share over 100% of the direct costs and that will be $100,733
Total UTD budget is approx. 195K (approx. 65K/yr)
Total budget including cost sharing is $400,838

Budget details are appended to this proposal.

Budget Justification:

The budget will support Dr. Thuraisingham half a month in the summer. She will use her startup funds to work at least one month per year in the summer.

The budget will support Dr. Khan half a month in the summer per year.

Dr. Harris will devote a few days consulting on the project and formulating scenarios.

UTD will employ 3 graduate students: 1.5 students on Task 1 and 1.5 students on Task 3.

GMU will support 1 student on Task 2.

Dr. Sandhu will spend at least one month per year on the project.

Dr. Thuraisingham will travel to Washington at least once a year and Dr. Sandhu will travel to Dallas at least once a year.

UTD

THE UNIVERSITY OF TEXAS AT DALLAS

BOX 830688 MP15 RICHARDSON, TEXAS 75083-0688
(972) 883-2313 FAX (972) 883-2310

OFFICE OF SPONSORED PROJECTS

May 25, 2005

AFOSR/PK
4015 Wilson Boulevard, Room 713
Arlington, VA 22203

SUBJECT: UT Dallas Proposal 050279

Dear Sir/Madame:

The University of Texas at Dallas is pleased to submit six (6) copies of the following proposal, including one copy signed by the principal investigator and an officer of the university:

TITLE:	Improving Trust and Reliability of Biometric Systems
PRINCIPAL INVESTIGATOR:	Bhavani Thuraisingham, Ph.D.
CO-PRINICIPAL INVESTIGATOR:	Latifur Khan, Ph.D.
AMOUNT REQUESTED:	$300,105

If you need additional information or assistance in finalizing the award, please do not hesitate to call Leslie Harper, Grant and Contract Specialist, Office of Sponsored Projects at area code (972) 883-2314 or via email at *leslie.harper@utdallas.edu*.

Sincerely,

Robert L. Lovitt
Senior Vice President for
Business Affairs

Enclosures

By signing this Signature Page, the Offeror represents and certifies compliance with the attached Certifications and Representations.

The full text of a solicitation provision may be accessed electonically at these: **http://farsite.hill.af.mil.**

SIGNATURE PAGE

NAME OF APPLICANT UNIVERSITY OF TEXAS AT DALLAS	RESEARCH TITLE INFORMATION OPERATIONS ACROSS INFOSPHERES
PRINTED NAME AND TITLE OF AUTHORIZED REPRESENTATIVE Robert L. Lovitt Sr. VP for Business Affairs	
SIGNATURE	DATE 05/27/2005
	Principal Investigator Bhavani Thuraisingham

I. NOTICE: The following solicitation provisions pertinent to this section are hereby incorporated by reference:

A. DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENT SOLICITATION PROVISIONS

252.209-7001 DISCLOSURE OF OWNERSHIP OR CONTROL BY THE GOVERNMENT OF A TERRORIST COUNTRY (SEP 2004)

II. NOTICE: The following solicitation provisions pertinent to this section are hereby incorporated in full text:

A. FEDERAL ACQUISITION REGULATION SOLICITATION PROVISIONS IN FULL TEXT

(1) 52.204-8 ANNUAL REPRESENTATIONS AND CERTIFICATIONS (JAN 2005)

(a)(1) If the clause at 52.204-7, Central Contractor Registration, is included in this solicitation, paragraph (b) of this provision applies. (Note: FAR 52.204-7 is included in all AFOSR contracts)

(2) If the clause at 52.204-7 is not included in this solicitation, and the offeror is currently registered in CCR, and has completed the ORCA electronically, the offeror may choose to use paragraph (b) of this provision instead of completing the corresponding individual representations and certifications in the solicitation. The offeror shall indicate which option applies by checking one of the following boxes:

[ ] (i) Paragraph (b) applies.

[X] (ii) Paragraph (b) does not apply and the offeror has completed the individual representations and certifications in the solicitation

(b) The offeror has completed the annual representations and certifications electronically via the Online Representations and Certifications Application (ORCA) website at http://orca.bpn.gov. After reviewing the ORCA database information, the offeror verifies by submission of the offer that the representations and certifications currently posted electronically have been entered or updated within the last 12 months, are current, accurate, complete, and applicable to this solicitation (including the business size standard applicable to the NAICS code referenced for this solicitation), as of the date of this offer and are incorporated in this offer by reference (see FAR 4.1201); except for the changes identified below [offeror to insert changes, identifying change by clause number, title, date]. These amended representation(s) and/or certification(s) are also incorporated in this offer and are current, accurate, and complete as of the date of this offer

FAR Clause	Title	Date	Change

Any changes provided by the offeror are applicable to this solicitation only, and do not result in an update to the representations and certifications posted on ORCA.

(2) 52.219-1 SMALL BUSINESS PROGRAM REPRESENTATIONS (MAY 2004)

(Note: Since the representation in subparagraph (b)(1) of this provision is not always complete in ORCA, please complete the following.)

(a)

(1) The North American Industry Classification System (NAICS) code for this acquisition is __**see table below**______________________.

(2) The small business size standard is _**see table below**______

R&D in the Physical, Engineering, and Life Sciences: **500 Employees**	**54171**
R&D in the Social Sciences and Humanities: **$5.0 Million**	**54172**

(3) The small business size standard for a concern which submits an offer in its own name, other than on a construction or service contract, but which proposes to furnish a product which it did not itself manufacture, is 500 employees.

(b) *Representations*

(1) The offeror represents as part of its offer that it [ ] is, [X] is not a small business concern

B. DEFENSE FAR SUPP SOLICITATION PROVISIONS IN FULL TEXT

252.225-7018 NOTICE OF PROHIBITION OF CERTAIN CONTRACTS WITH FOREIGN ENTITIES FOR THE CONDUCT OF BALLISTIC MISSILE DEFENSE RDT&E (JAN 1997) (Applicable to MDA efforts only)

(a) *Definitions.*

(1) "Competent" means the ability of an offeror to satisfy the requirements of the solicitation. This determination is based on a comprehensive assessment of each offeror's proposal including consideration of the specific areas of evaluation criteria in the relative order of importance described in the solicitation.

(2) "Foreign firm" means a business entity owned or controlled by one or more foreign nationals or a business entity in which more than 50 percent of the stock is owned or controlled by one or more foreign nationals.

(3) "U.S. firm" means a business entity other than a foreign firm.

(b) Except as provided in paragraph (c) of this provision, the Department of Defense will not enter into or carry out any contract, including any contract awarded as a result of a broad agency announcement, with a foreign government or firm if the contract provides for the conduct of research, development, test, or evaluation in connection with the Ballistic Missile Defense Program. However, foreign governments and firms are encouraged to submit offers, since this provision is not intended to restrict access to unique foreign expertise if the contract will require a level of competency unavailable in the United States.

(c) This prohibition does not apply to a foreign government or firm if—

(1) The contract will be performed within the United States;

(2) The contract is exclusively for research, development, test, or evaluation in connection with antitactical ballistic missile systems;

(3) The foreign government or firm agrees to share a substantial portion of the total contract cost. The foreign share is considered substantial if it is equitable with respect to the relative benefits that the United States and the foreign parties will derive from the contract. For example, if the contract is more beneficial to the foreign party, its share of the costs should be correspondingly higher; or

(4) The U.S. Government determines that a U.S. firm cannot competently perform the contract at a price equal to or less than the price at which a foreign government or firm can perform the contract.

(d)The Offeror [ ] is [X] is not a U.S. firm

252.227-7017 IDENTIFICATION AND ASSERTION OF USE, RELEASE, OR DISCLOSURE RESTRICTIONS (JUN 1995)

(a) The terms used in this provision are defined in following clause or clauses contained in this solicitation--

(1) If a successful offeror will be required to deliver technical data, the Rights in Technical Data--Noncommercial Items clause, or, if this solicitation contemplates a contract under the Small Business Innovative Research Program, the Rights in Noncommercial Technical Data and Computer Software--Small Business Innovative Research (SBIR) Program clause.

(2) If a successful offeror will not be required to deliver technical data, the Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation clause, or, if this solicitation contemplates a contract under the Small Business Innovative Research Program, the Rights in Noncommercial Technical Data and Computer Software--Small Business Innovative Research (SBIR) Program clause.

(b) The identification and assertion requirements in this provision apply only to technical data, including computer software documentation, or computer software to be delivered with other than unlimited rights. For contracts to be awarded under the Small Business Innovative Research Program, the notification and identification requirements do not apply to technical data or computer software that will be generated under the resulting contract. Notification and identification is not required for restrictions based solely on copyright

(c) Offers submitted in response to this solicitation shall identify, to the extent known at the time an offer is submitted to the Government, the technical data or computer software that the Offeror, its subcontractors or suppliers, or potential subcontractors or suppliers, assert should be furnished to the Government with restrictions on use, release, or disclosure.

(d) The Offeror's assertions, including the assertions of its subcontractors or suppliers or potential subcontractors or suppliers shall be submitted as an attachment to its offer in the following format, dated and signed by an official authorized to contractually obligate the Offeror:

Identification and Assertion of Restrictions on the Government's Use, Release, or Disclosure of Technical Data or Computer Software.

The Offeror asserts for itself, or the persons identified below, that the Government's rights to use, release, or disclose the following technical data or computer software should be restricted:

Technical Data or Computer Software to be Furnished With Restrictions*	Basis for Assertion**	Asserted Rights Category***	Name of Person Asserting Restrictions****
(LIST)*****	(LIST)	(LIST)	(LIST)
NONE			

*For technical data (other than computer software documentation) pertaining to items, components, or processes developed at private expense, identify both the deliverable technical data and each such item, component, or process. For computer software or computer software documentation identify the software or documentation.

**Generally, development at private expense, either exclusively or partially, is the only basis for asserting restrictions. For technical data, other than computer software documentation, development refers to development of the item, component, or process to which the data pertain The Government's rights in computer software documentation generally may not be restricted. For computer software, development refers to the software Indicate whether development was accomplished exclusively or partially at private expense. If development was not accomplished at private expense, or for computer software documentation, enter the specific basis for asserting restrictions.

***Enter asserted rights category (e.g., government purpose license rights from a prior contract, rights in SBIR data generated under another contract, limited, restricted, or government purpose rights under this or a prior contract, or specially negotiated licenses).

****Corporation, individual, or other person, as appropriate.

*****Enter "none" when all data or software will be submitted without restrictions.

Date 5/27/05

Printed Name and Title Robert L. Lovitt, Sr VP for Business Affairs

Signature

(End of identification and assertion)

(e) An offeror's failure to submit, complete, or sign the notification and identification required by paragraph (d) of this provision with its offer may render the offer ineligible for award

(f) If the Offeror is awarded a contract, the assertions identified in paragraph (d) of this provision shall be listed in an attachment to that contract Upon request by the Contracting Officer, the Offeror shall provide sufficient information to enable the Contracting Officer to evaluate any listed assertion.

252.247-7022 REPRESENTATION OF EXTENT OF TRANSPORTATION BY SEA (AUG 1992)

(a) The Offeror shall indicate by checking the appropriate blank in paragraph (b) of this provision whether transportation of supplies by sea is anticipated under the resultant contract. The term "supplies" is defined in the Transportation of Supplies by Sea clause of this solicitation.

(b) Representation. The Offeror represents that it--

[ ] Does anticipate that supplies will be transported by sea in the performance of any contract or subcontract resulting from this solicitation.

[X] Does not anticipate that supplies will be transported by sea in the performance of any contract or subcontract resulting from this solicitation

(c) Any contract resulting from this solicitation will include the Transportation of Supplies by Sea clause. If the Offeror represents that it will not use ocean transportation, the resulting contract will also include the Defense FAR Supplement clause at 252 247-7024, Notification of Transportation of Supplies by Sea.

SUMMARY PROPOSAL BUDGET FORM

FOR AFOSR USE ONLY

ORGANIZATION The University of Texas at Dallas	CAGE CODE 74-R-0068		DURATION (MONTHS) Proposed | Granted
PRINCIPAL INVESTIGATOR/PROJECT DIRECTOR Bhavani Thuraisingham, Ph.D.		AWARD NO	

A. SENIOR PERSONNEL: PI/PD, Co-PI's, Faculty and Other Senior Associates (List each separately with title, A.7. Show number in brackets)	AFOSR-Funded Person-months **(Monthly or hourly rate) **RATE	%	CF	MOS	Funds Cost Shared Proposer	Funds Requested from AFOSR
1. Bhaveni Thuraisingham, Ph.D. (PI)	3600/mo	.5			11403	11403
2. Latifur Khan, Ph.D. (Co-PI)	2200/mo	.5		1	3395	3396
3						
4. ( ) OTHERS (LIST INDIVIDUALLY ON BUDGET EXPLANATION PAGE)						
5. ( ) TOTAL SENIOR PERSONNEL (1-6)						
B. OTHER PERSONNEL (SHOW NUMBERS IN BRACKETS)						
1. ( ) POST DOCTORAL ASSOCIATES						
2. ( ) OTHER PROFESSIONALS (TECHNICIAN, PROGRAMMER, ETC.)						
3. (1) GRADUATE STUDENTS	2916/mo				54750	54750
4. ( ) UNDERGRADUATE STUDENTS						
5. ( ) SECRETARIAL – CLERICAL (IF CHARGED DIRECTLY)						
6. ( ) OTHER: (PROVIDE EXPLANATION)						
TOTAL SALARIES AND WAGES (A + B)						
C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS) PLEASE PROVIDE DETAIL OF THE CALCULATION ON AN ATTACHMENT IF NOT APPLIED DIRECTLY TO THE SALARIES TOTAL - REF SECTION 2.12.7.					17488	17468
TOTAL SALARIES, WAGES AND FRINGE BENEFITS (A + B + C)					67017	67017
D. EQUIPMENT (LIST ITEM AND DOLLAR AMOUNT FOR EACH ITEM EXCEEDING $5,000) (PLEASE ATTACH DETAIL AND VENDOR QUOTES) - REF 2.12.12						
TOTAL EQUIPMENT						
E. TRAVEL 1. DOMESTIC (INCL. CANADA, MEXICO AND U.S. POSSESSIONS)					2250	2250
2. FOREIGN (PROVIDE PER DIEM, DAYS OF STAY, AND PURPOSE)						
F. TUITION REF 2.12.13						
( ) TOTAL PARTICIPANT COSTS						
G. OTHER DIRECT COSTS						
1. SUPPLIES/MATERIALS					390	390
2. COMPUTER						
3. CONSULTANT SERVICES (provide detail)						
4. PUBLICATIONS					370	370
5. COMM'S/SHIPPING						
6. SUBCONTRACT (provide budget)						150,000
7. OTHER (provide detail)						
TOTAL OF OTHER DIRECT COSTS						
H. TOTAL DIRECT COSTS (A THROUGH G)					92,127	242,127
I. FACILITIES AND ADMINISTRATION EXPENSE (overhead) - specify the rate and base below)						57,978
TOTAL FACILITIES AND ADMINISTRATION EXPENSES						
J. TOTAL DIRECT EXPENSES AND FACILITIES AND ADMINISTRATION EXPENSES(H + I)					92,127	300,105

	Rate (49.5%)	Base ($117,127)	Total ($57,978)
Overhead			
G&A			
Fringe Benefits			
FCCOM			

K. RESIDUAL FUNDS (IF FOR FURTHER SUPPORT OF CURRENT PROJECT SEE GPG II.D.7.j.)		
L. AMOUNT OF THIS REQUEST (J) OR (J MINUS K)	$100,733	$300,105

M. COST-SHARING: PROPOSED LEVEL $100,733 AGREED LEVEL IF DIFFERENT: $

* APPROVED PURCHASING SYSTEM? YES □ NO X

IF YES, DATE OF ONR APPROVAL AND EXPIRATION

PI/PD TYPED NAME AND SIGNATURE* DATE

Bhavani Thuraisingham

ORG. REP. TYPED NAME & SIGNATURE* DATE 5/27/05

Robert L. Lovitt

FOR AFOSR USE ONLY

FACILITIES AND ADMINISTRATION EXPENSES VERIFICATION		
Date Checked	Date of Rate Sheet	Initials-ORG

Attachment 5

CERTIFICATIONS REGARDING DEBARMENT; SUSPENSION AND OTHER RESPONSIBILITY MATTERS; RESTRICTIONS ON LOBBYING; DRUG-FREE WORKPLACE REQUIREMENTS; THE CIVIL RIGHTS ACT OF 1964; AND THE REHABILITATION ACT OF 1973

Applicants should refer to the regulations cited below to determine the certification to which they are required to attest. Applicants should also review the instructions for certification requirement under 32 CFR Part 25, "Government-wide Debarment and Suspension (Nonprocurement)"; 32 CFR Part 28, "New Restrictions on Lobbying"; 32 CFR Part 25, "Government-wide Requirements for Drug-Free Workplace (Grants)" and 32 CFR 56, DoD Implementation of the Rehabilitation Act of 1973. The certification shall be treated as a material representation of fact upon which reliance will be placed when the Air Force Office of Scientific Research determines to award the covered transaction, grant, or cooperative agreement.

CERTIFICATION REGARDING DEBARMENT, SUSPENSION, AND OTHER RESPONSIBILITY MATTERS - PRIMARY COVERED TRANSACTIONS 32 CFR Part 25, Appendix A

1. The prospective primary participant certifies to the best of its knowledge and belief, that it and its principals:

a. Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any Federal department or agency;

b. Have not within a three-year period preceding this proposal been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State, or local) transaction or contract under a public transaction; violation of Federal or State antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;

c. Are not presently indicted for or otherwise criminally or civilly charged by a governmental entity (Federal, State, or local) with commission of any of the offenses enumerated in paragraph 1b of this certification; and

d. Have not within a three-year period preceding this application/proposal had one or more public transactions (Federal, State, or local) terminated for cause or default.

2. Where the prospective primary participant is unable to certify to any of the statements in this certification, such prospective participant shall attach an explanation to the proposal.

LOBBYING CERTIFICATION FOR CONTRACTS, GRANTS, LOANS, AND COOPERATIVE AGREEMENTS

The undersigned certifies, to the best of his or her knowledge and belief, that:

1. No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.

2. If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.

3. The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

The certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by section 1352, Title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

GRANTEE CERTIFICATION REGARDING DRUG-FREE WORKPLACE REQUIREMENTS

Alternate I. (Grantees Other Than Individuals)

A. The grantee certifies that it will or will continue to provide a drug-free workplace by:

(a) Publishing a statement notifying employees that the unlawful manufacture, distribution, dispensing, possession, or use of a controlled substance is prohibited in the grantee's workplace and specifying the actions that will be taken against employees for violation of such prohibition;

fdf(b) Establishing an ongoing drug-free awareness program to inform employees about -

(1) The dangers of drug abuse in the workplace;

(2) The grantee's policy of maintaining a drug-free workplace;

(3) Any available drug counseling, rehabilitation, and employee assistance programs; and

(4) The penalties that may be imposed upon employees for drug abuse violations occurring in the workplace;

(c) Making it a requirement that each employee to be engaged in the performance of the grant be given a copy of the statement required by paragraph (a);

(d) Notifying the employee in the statement required by paragraph (a) that, as a condition of employment under the grant, the employee will -

(1) Abide by the terms of the statement; and

(2) Notify the employer in writing of his or her conviction for a violation of a criminal drug statute occurring in the workplace no later than five calendar days after such conviction;

(e) Notifying the agency in writing, within ten calendar days after receiving notice under subparagraph (d)(2) from an employee or otherwise receiving actual notice of such conviction. Employers of convicted employees must provide notice, including position title, to every grant officer or other designee on whose grant activity the convicted employee was working, unless the Federal agency has designated a central point for receipt of such notices. Notice shall include the identification number(s) of each affected Grant;

(f) Taking one of the following actions, within 30 calendar days of receiving notice under subparagraph (d)(2), with respect to any employee who is so convicted -

(1) Taking appropriate personnel action against such an employee, up to and including termination, consistent with the requirements of the Rehabilitation Act of 1973, as amended; or

(2) Requiring such employee to participate satisfactorily in a drug abuse assistance or rehabilitation program approved for such purposes by a Federal, State, or local health, law enforcement, or other appropriate agency;

(g) Making a good faith effort to continue to maintain a drug-free

B The grantee may insert in the space provided below the site(s) for the performance of work done in connection with the specific grant:

Place of Performance (Street address, city, county, state, zip code)

2601 N FLOYD RD RICHARDSON TX 75080

Check □ if there are workplaces on file that are not identified here

CIVIL RIGHTS ACT OF 1964

The prospective recipient certifies that it is complying with all requirements set forth in Title VI of the Civil Rights Act of 1964, as implemented by 32 CFR 195, concerning nondiscrimination in activities under the resultant agreement based on race, color, or national origin

REHABILITATION ACT OF 1973

The prospective recipient certifies that it is complying with the requirements of section 504 of the Rehabilitation Act of 1973, as implemented by 32 CFR 56, concerning access for people with disabilities in recipient programs and activities, including but not limited to those under any resultant agreement

As the duly authorized representative of the applicant, I hereby make the above certifications on behalf of the applicant

NAME OF APPLICANT AND TAXPAYER IDENTIFICATION NUMBER (TIN). UNIVERSITY OF TEXAS AT DALLAS TIN: 75-1305566	RESEARCH TITLE **Information Operations Across Infospheres**
PRINTED NAME, TITLE AND SIGNATURE OF AUTHORIZED REPRESENTATIVE Robert L. Lovitt, Sr VP for Business Affairs	DATE 5/27/05
PR NUMBER:	
PRINCIPAL INVESTIGATOR: Bhavani Thuraisingham	
NEGOTIATOR: LESLIE HARPER	

OMB No 0925-0418
Approved for use through 01/31/2001

Protection of Human Subjects
Assurance Identification/Certification/Declaration
(Common Federal Rule)

Policy: Research activities involving human subjects may not be conducted or supported by the Departments and Agencies adopting the Common Rule (56FR28003, June 18, 1991) unless the activities are exempt from or approved in accordance with the common rule. See section 101(b) the common rule for exemptions. Institutions submitting applications or proposals for support must submit certification or appropriate Institutional Review Board (IRB) review and approval to the Department or Agency in accordance with the common rule. Institutions with an assurance of compliance that covers the research to be conducted on file with the Department, Agency, or the Department of Health and Human Services (HHS) should submit certification of IRB review and approval with each application or proposal unless otherwise advised by the Department or Agency. Institutions which do not have such an assurance must submit an assurance and certification of IRB review and approval within 30 days of a written request from the Department or Agency.

1. Request Type
☒ ORIGINAL
□ FOLLOWUP
□ EXEMPTION

2. Type of Mechanism
☒ GRANT □ CONTRACT
□ FELLOWSHIP
□ COOPERATIVE AGREEMENT
□ OTHER: ____________

3. Name of Federal Department or Agency and, if known, Application or Proposal Identification No.
AIR FORCE OFFICE OF SCIENTIFIC RESEARCH

4. Title of Application or Activity
Information Operations Across Infospheres

5. Name of Principal Investigator, Program Director, Fellow, or Other
Bhavani Thuraisingham

6. Assurance Status of this Project *(Respond to one of the following)*

☒ This Assurance, on file with Department of Health and Human Services, covers this activity:
Assurance identification no. M-1059 IRB identification no. ____________

□ This Assurance, on file with *(agency/dept)* ______________________________, covers this activity
Assurance identification no ________ IRB identification no. ________ *(if applicable)*

□ No assurance has been filed for this project. This institution declares that it will provide an Assurance and Certification of IRB review and approval
upon request

□ Exemption Status: Human subjects are involved, but this activity qualifies for exemption under Section 101(b), paragraph __________

7. Certification of IRB Review (Respond to one of the following IF you have an Assurance on file)

□ This activity has been reviewed and approved by the IRB in accordance with the common rule and any other governing regulations or subparts on *(date)* ________ by: □ Full IRB Review or □ Expedited Review

□ This activity contains multiple projects, some of which have not been reviewed. The IRB has granted approval on condition that all projects covered by the common rule will be reviewed and approved before they are initiated and that appropriate further certification will be submitted.

8. Comments
Regarding question 7, this project will have no human subjects and IRB Review is not relevant.

9. The official signing below certifies that the information provided above is correct and that, as required, future reviews will be performed and certification will be provided.

10. Name and Address of Institution
The University of Texas at Dallas
P.O. Box 830688, MP15
Richardson, TX 75083-0688

11. Phone No. *(with area code)*
(972) 883-2213

12. Fax No. *(with area code)*
(972) 883-2212

13. Name of Official
Robert L. Lovitt

14. Title
Sr. VP for Business Affairs

15. Signature

16. Date
5/27/05

Authorized for local Reproduction
HHS/PHS/NIH

OPTIONAL FORM 310 (Rev. 1-98)

Sponsored by

Public reporting burden for the collection of information is estimated to average less than an hour per response. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid OMB control number. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to: NIH, Project Clearance Office, 6701 Rockledge Drive MSC 7730, Bethesda Md 20892-7730, ATTN: PRA 0925-0418. *Do not return the completed form to this address*

The National Environmental Policy Act of 1969 (NEPA) requires Federal agencies to consider potential environmental concerns of major federal undertakings. This includes research projects funded by the Air Force Office of Scientific Research (AFOSR). Under the Air Force Environmental Impact Analysis Process, all projects must have an environmental assessment or environmental impact statement completed UNLESS they qualify for a categorical exclusion from this requirement. In order to qualify for this categorical exclusion, proposed research must be normal and routine basic or applied research confined to the laboratory and in compliance with all safety, environmental, and natural resource conservation laws. The following documentation must be completed in order to assist AFOSR in determining whether the proposed research meets the criteria for such categorical exclusion.

The University of Texas at Dallas and Bhavani Thuraisingham
(Name of Proposing Institution) (Name of Investigator)
hereby certify as follows:

1. All research to be performed under the proposal for research Information Operations Across Infospheres
(Research Title)

will be confined to the laboratory, except as disclosed below:

N/A

2. All research identified in number 1 above, will be conducted in compliance with all safety, environmental, and natural resource conservation laws, except as disclosed below

N/A

3. The proposed research does not involve major construction or remodeling of buildings used as research or test facilities.

4. Any additional information that will assist AFOSR in accomplishing the required environmental determination:

N/A

The parties signing this certification below understand that the Air Force Office of Scientific Research will rely on the certification in making determinations under the Air Force Environmental Impact Analysis Process and whether the proposed research qualifies for a categorical exclusion.

05/27/2005
(Signature of Authorized Official of the Institution) (Date)

05/27/2005
(Signature of Principal Investigator) (Date)

George Mason University

Fairfax, Virginia 22030-4444

May 27, 2005

Ms. Carolyn Ivey
Assistant Director
Office of Sponsored Projects
University of Texas - Dallas
2601 N. Floyd Road, MP15
Richardson, TX 75080

RE: Subcontract from University of Texas - Dallas
Title: Information Operation Across Infospheres
Prime: Air Force Office of Scientific Research

Dear Ms. Ivey:

George Mason University (GMU) looks forward to collaborating with the University of Texas - Dallas on the above-cited Subcontract. The GMU's principal investigator is Dr. Ravi Sandhu, Department of Information & Software Engineering, George Mason University. Enclosed please find GMU's Statement of Work and Budget.

GMU understands that any subcontract resulting from this proposal will include those clauses required by the prime contract, all clauses required by law or on the date of execution of the subcontract, and any other mutually agreeable clauses, terms, and conditions except those inconsistent with OMB Circular A-110 (Grants and Agreements with Institutions of Higher Education, etc.) and OMB Circular A-21 (Cost Principles for Educational Institutions), or those not allowed by Virginia state law.

In accordance with OMB Circular A-21, cost reimbursement and fixed price contracts are the appropriate contract vehicles for institutions of higher education. Since not all government-contracting officers are experienced in contracting with universities, GMU requests that the GMU Office of Sponsored Programs be notified should negotiations begin with the government regarding an award of a contract. Notification of GMU during initial negotiations will ensure that the contract contains appropriate clauses for universities and that the execution of a subsequent subcontract is facilitated.

If you have any questions regarding the technical content of this proposal, please contact Dr. Snadhu at 703/993-1659or sandhu@gmu.edu. Questions regarding GMU policies and procedures may be directed to Patricia M. Carcamo, Office of Sponsored Programs, at 703/993-2987.

Sincerely,

Karen G. Cohn

Karen G. Cohn
Associate Director, Pre-Award
Office of Sponsored Programs

cc: R. Sandhu

Statement of work

Information Operation Across Infospheres

George Mason University will perform task 2 of this project in Years 1, 2 and 3.

Task 2: Access Control (GMU; Year 1, Year 2 and Year 3)

We will investigate the use of Role-based and Usage Control policies in the collaborative environment. We will specify the policies and develop techniques to enforce the policies across infospheres. Prototypes for RBAC and UCON techniques will be demonstrated.

Task 2 Deliverables:

Year 1: Interim Report

Year 2: Interim Report

Year 2: Final Report, Proof of Concept Demonstration

SUMMARY PROPOSAL BUDGET FORM

FOR AFOSR USE ONLY

ORGANIZATION George Mason University	CAGE CODE 7X764		DURATION (MONTHS) 36 Months
			Proposed | Granted
PRINCIPAL INVESTIGATOR/PROJECT DIRECTOR Ravi Sandhu		AWARD NO.	

A. SENIOR PERSONNEL: PI/PD, Co-PI's, Faculty and Other Senior Associates (List each separately with title, A.7 Show number in brackets)	AFOSR-Funded Person-months **(Monthly or hourly rate)			Funds Cost Shared Proposer	Funds Requested from AFOSR
	**RATE	% OF	MOS		
1. Dr. Ravi Sandhu – PI		13%	1.66	$	$ 61,831
2.					
3					
4. ( ) OTHERS (LIST INDIVIDUALLY ON BUDGET EXPLANATION PAGE)					
5. ( ) TOTAL SENIOR PERSONNEL (1-6)					
B. OTHER PERSONNEL (SHOW NUMBERS IN BRACKETS)					
1 ( ) POST DOCTORAL ASSOCIATES					
2. ( ) OTHER PROFESSIONALS (TECHNICIAN, PROGRAMMER, ETC.)					
3. (1) GRADUATE STUDENTS					$ 13,681
4. ( ) UNDERGRADUATE STUDENTS					
5. ( ) SECRETARIAL – CLERICAL (IF CHARGED DIRECTLY)					
6. ( ) OTHER: (PROVIDE EXPLANATION)					
TOTAL SALARIES AND WAGES (A + B)					
C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS) PLEASE PROVIDE DETAIL OF THE CALCULATION ON AN ATTACHMENT IF NOT APPLIED DIRECTLY TO THE SALARIES TOTAL – REF SECTION 2.12.7.					$ 18,698
TOTAL SALARIES, WAGES AND FRINGE BENEFITS (A + B + C)					$ 95,193
D. EQUIPMENT (LIST ITEM AND DOLLAR AMOUNT FOR EACH ITEM EXCEEDING $5,000) (PLEASE ATTACH DETAIL AND VENDOR QUOTES) - REF 2.12.12					
TOTAL EQUIPMENT					
E. TRAVEL 1. DOMESTIC (INCL. CANADA, MEXICO AND U.S. POSSESSIONS)					$ 6,473
2. FOREIGN (PROVIDE PER DIEM, DAYS OF STAY, AND PURPOSE)					
F. TUITION REF 2.12.13					
( ) TOTAL PARTICIPANT COSTS					
G. OTHER DIRECT COSTS					
1. SUPPLIES/MATERIALS					$1,600
2. COMPUTER					
3. CONSULTANT SERVICES (provide detail)					
4. PUBLICATIONS					
5. COMM'S/SHIPPING					
6. SUBCONTRACT (provide budget)					
7. O¹THER (provide detail) Photocopy					$1,000
TOTAL OF OTHER DIRECT COSTS					$8,073
H. TOTAL DIRECT COSTS (A THROUGH G)					$104,166
I. FACILITIES AND ADMINISTRATION EXPENSE (overhead)- specify the rate and base below)					
TOTAL FACILITIES AND ADMINISTRATION EXPENSES					
J. TOTAL DIRECT EXPENSES AND FACILITIES AND ADMINISTRATION EXPENSES(H + I)					$45,833
K. RESIDUAL FUNDS (IF FOR FURTHER SUPPORT OF CURRENT PROJECT SEE GPG II.D.7.j.)					
L. AMOUNT OF THIS REQUEST (J) OR (J MINUS K)					$150,000

	Rate (%)	Base ($)	Total ($)
	44% of MTDC	$104,166	$45,833
Overhead			
G&A			
Fringe Benefits			
FCCOM			

M. COST-SHARING: PROPOSED LEVEL $ AGREED LEVEL IF DIFFERENT: $

* APPROVED PURCHASING SYSTEM? YES □ NO ☒

IF YES, DATE OF ONR APPROVAL AND EXPIRATION ____________

PI/PD TYPED NAME AND SIGNATURE* Ravi Sandhu

Ravi Sandhu

DATE 5/27/05

ORG REP TYPED NAME & SIGNATURE*

Karen G. Cohn, Associate Director Karen G. Cohn

DATE 5/27/05

FOR AFOSR USE ONLY

FACILITIES AND ADMINISTRATION EXPENSES VERIFICATION

Date Checked	Date of Rate Sheet	Initials-CRG

Attachment 5

George Mason University
4400 University Drive
Fairfax, VA 22030

University of Texas at Dallas
Subcontract from Air Force Office of Scientific Research
08/01/2005 - 07/31/2008

		YEAR ONE	GMU IN-KIND	YEAR TWO	GMU IN-KIND	YEAR THREE	GMU IN-KIND	TOTAL
A. PERSONNEL								
1 Faculty - Fiscal Plan	FTE							
PI: Dr. Ravi Sandhu	0.13	20,566	0	21,594	0	22,674	0	64,834
2 Faculty - Summer	FTE							
PI: Dr. Ravi Sandhu	0.00	0	0	0	0	0	0	0
3 Students (AY)	No.							
GRA - Doctoral (20 Hrs/Wk)	0	0	0	0	0	0	0	0
Students (SUM)								
GRA - Doctoral (20 Hrs/Wk)	1	4,333	0	4,550	0	4,778	0	13,661
TOTAL PERSONNEL		24,899	0	26,144	0	27,452	0	78,495
B FRINGE BENEFITS								
@ 24.14% (AY & CY Faculty)		4,965	0	5,213	0	5,474	0	15,652
@ 7.65% (GRA's & Summer Faculty)		332	0	348	0	366	0	1,046
TOTAL FRINGE		5,297	0	5,561	0	5,840	0	16,698
C TRAVEL				0				
1 Domestic Travel		2,160	0	2,160	0	2,153	0	6,473
TOTAL TRAVEL		2,160	0	2,160	0	2,153	0	6,473
D SUPPLIES								
1 General Office Supplies		500	0	500	0	500	0	1,500
TOTAL SUPPLIES		500	0	500	0	500	0	1,500
E. EQUIPMENT								
1 Computers		0	0	0	0	0	0	0
TOTAL EQUIPMENT		0	0	0	0	0	0	0
F. OTHER DIRECT COSTS								
1 Photocopy		0	0	500	0	500	0	1,000
2 Tuition GRA(s)								
Doctoral - OutState: 12 Credit Hrs @ $715/Hr		0	0	0	0	0	0	0
TOTAL OTHER		0	0	500	0	500	0	1,000
TOTAL DIRECT COSTS		32,856	0	34,865	0	36,445	0	104,166
G INDIRECT COSTS								
44% Modified Total Direct Costs		14,457	0	15,341	0	16,036	0	45,834
Provisional Indirect Rate as of 07/01/2004								
TOTAL COSTS		47,313	0	50,206	0	52,481	0	150,000

GMU IN-KIND COST SHARE: 0%

TOTAL DIRECT COSTS REQUESTED FROM SPONSOR	104,166
TOTAL INDIRECT COSTS REQUESTED FROM SPONSOR	45,834
TOTAL REQUESTED FROM SPONSOR	150,000
TOTAL GMU IN-KIND	0
TOTAL GMU UNRECOVERED INDIRECT	0
TOTAL PROGRAM COSTS	150,000

Salaries and wages are estimates only. Actual salaries and wages will be paid in accordance with University policy.

Tuition and fees are budgeted at Out/State rates. Actual charges will be made according to individual domiciliary classification.

Budget preparation:

S:\BudTeam\ITE\ISE\Sandhu, Ravi\AFRL Subcontract to UTD

Patricia M. Carcamo
2/3/2005