Information Security Scholarship-for-Service at The University of Arizona

PI: Dr. Hsinchun Chen, McClelland Professor of Management Information Systems, The University of Arizona
Co-PIs: Dr. Paulo Goes, Dr. Mark Patton, Ms. Cathy Larson; The University of Arizona

Project Description

I. Introduction

Cybersecurity and Information Assurance are critical to ensuring the integrity and availability demands of a modern, globally-networked infrastructure. Information Security (Infosec) is one of the core areas of information management, and hence a vital component to a solid information systems curriculum. To support the goal of developing well-trained, expert information security professionals, the Management Information Systems (MIS) Department of The University of Arizona (UA) has been designated by the National Security Agency (NSA) and the Department of Homeland Security as a Center of Academic Excellence in Information Assurance Education (CAE-IAE). In this proposal we describe our detailed plan to build an Information Security Scholarship-for-Service Program at the University of Arizona especially aimed at recruiting from across the state, with particular emphasis on minority recruitment and retention in order to help fulfill NSF, Federal, Arizona, and University of Arizona goals.

The MIS department has unique characteristics and faculty expertise which make it particularly suitable for managing a Federal Cyber Service Scholarship for Service (SFS) program. The department is renowned for its consistent ranking in the top five MIS programs in the country (*U.S. News and World Report*) for over 20 years, an achievement matched only by MIT and Carnegie-Mellon; currently, the UA program is ranked third. The PI, Dr. Hsinchun Chen, is McClelland Professor of Management Information Systems, and has over twenty years' experience in educating and mentoring undergraduate and graduate students through the MIS program. As the Director of the Artificial Intelligence Lab, he also has over fifteen years' experience as a successful PI for numerous security-related research projects funded by the National Science Foundation, National Institute of Justice, Department of Homeland Security, Department of Defense, and other agencies and entities. He is also the founder of the IEEE Intelligence and Security Informatics conferences, held in various locations world-wide since 2003 (more details on this conference can be found in a later section), and is the founding editor of the new Springer journal, *Security Informatics*. Dr. Mark Patton and Dr. Paulo Goes, co-PIs, are, like PI Chen, members of the Information Assurance and Security Education Center and carry significant responsibility for the administration of and teaching in the current program. The department is also home to the "National Center for Border Security and Immigration" (Borders) a Department of Homeland Security Center of Excellence. Dr. Jay Nunamaker, a UA Regents and Soldwedel Professor of MIS and Director of the Center for the Management of Information (CMI) (and a member of the CAE-IAE), is the Director and PI for the Borders program, which focuses on five security-related areas: detection; networks; fusion; risk; and training, testing and commercialization. Dr. Nunamaker will serve as a faculty mentor. Both Chen and Nunamaker carry current security clearances.

Our approach to managing the program is deliberately cross-disciplinary. In addition to faculty from MIS, Dr. Salim Hariri of the Electrical and Computer Engineering department will also serve as Co-PI. Dr. Hariri brings a wealth of experience in cyber- and network security. Faculty members from Computer Science have also signed on as faculty mentors. This broad inclusiveness will, we believe, improve our chances of successful recruitment into the program as students will be encouraged to minor in or otherwise take classes in any of these areas (outside of their major) in order to broaden their understanding of information security.

Leveraging the departments' unique research strengths in security and security informatics, combined with our coursework, faculty expertise, CNSS certificate program in Information Security, and status as a Center of Academic Excellence in Information Assurance Education, we propose an NSF SFS program to prepare undergraduate and graduate students for Federal Cyber Service. The program will focus on recruiting SFS eligible domestic students interested in government service from the undergraduate body and statewide community and tribal colleges, and on promising undergraduate students who have completed their degree at a minority institution as recognized by the Department of Educations' List who seek a master's or PhD. degree before entering the workforce. Our proposed program has a specific focus on and detailed plans for minority recruitment, in order to support NSF (and university) aims to increase minority recruitment and ultimately retention in the U.S. technology and science sectors. We will also leverage and expand our post-graduation placement services in order to help graduates address the service requirements of their scholarships.

The growing need for and demands upon security professionals are highlighted by the fact that the Association for Computing Machinery (ACM) and the Association for Information Systems (AIS) released new information systems curriculum guidelines in May 2010 that specifically addressed emerging needs. In addition to identifying the needs for security training in existing IS courses, the guidelines identify "Securing Data and Infrastructure" and "Understanding, Managing and Controlling IT Risks" as two stand-alone high-level IS capabilities and include a suggested curriculum for a dedicated security and risk management course (Topi, et al. 2010). The biggest challenge facing employers is finding employees with the right security skills, including operations security, information security risk management, and security management practices (Goodwin 2010), thus proving the SFS program an opportune and timely solution to a challenging problem government agencies face in attracting qualified security candidates.

II. Project Objectives and Plans

The Program encompasses several important areas of activity, including: recruitment; eligibility verification and selection; student mentoring and development (including independent research study); coursework; assessment of student progress; internship and post-graduation placement assistance; and program assessment and evaluation. Each area is addressed below.

A. Recruitment

We will implement a three pronged approach to recruitment to fulfill objectives for undergraduate, masters, and PhD students. Our specific focus is on building a program for Arizona and we aim to recruit very heavily across the state, going further into the Southwest if needed to further our goals. The target objectives are to recruit five undergraduate, four masters, and two Ph.D. students each year for the first three years, and five undergraduate and five Masters Students in the fourth year. Undergraduate students will receive two years of support, Masters Students will receive three semesters of support, which is the duration of the master's program, and PhD students will receive three years of support. Over the 5 years of the program, 45 students will progress through the Scholarship-for-Service program.

The distribution of scholarships is based on the MIS department's current distribution of undergraduate, graduate, and PhD students and the ability to recruit a select group of students meeting all the program requirements and interested in government service upon graduation. The department has large undergraduate and graduate programs with new 2011 academic-year classes of 114 undergraduate students, 90 Master's students, and 9 PhD Student's.

Undergraduate recruiting will include direct recruiting from Eller College of Business second year students, as well as recruiting based on site visits to select members of Arizona's twenty-one community and Tribal colleges (Table 1). Arizona's seven Hispanic Serving institutions and two Tribal Colleges will be specifically targeted every year to ensure suitable minority representation. In addition, military personnel who have sufficient college credit to apply for admissions at the junior level will be solicited for enrollment from Arizona's seven military bases (Table 2). This broad approach should bring a diverse set of applicants including minority applicants who are also comfortable with the program requirements for government service following completion of the degree program.

Arizona Community Colleges	Primarily Serves	U.S. Minority Serving Status (2010 FTE HS % UG)
Arizona Western College	Yuma County	Hispanic Serving (57.5%)
Central Arizona College	Pinal County	Hispanic Serving (26.7%)
Cochise College	Cochise County	Hispanic Serving (42.1%)
Coconino Community College	Coconino County	
Diné College	Navajo Nation	Tribal College
Eastern Arizona College	Graham County	
Chandler-Gilbert Community College	Maricopa County	
Estrella Mountain Community College		Hispanic Serving (38.5%)
GateWay Community College		Hispanic Serving (26.6%)
Glendale Community College		Hispanic Serving (26.4%)
Mesa Community College		
Paradise Valley Community College		
Phoenix College		
Rio Salado Community College		
Scottsdale Community College		
South Mountain Community College		Hispanic Serving (33.6%)
Mohave Community College	Mohave County	
Northland Pioneer College	Navaho & Apache County	
Pima Community College	Pima County	Hispanic Serving (32.5%)
Tohono O'odham Community College	Tohono O'odham Nation	Tribal College
Yavapai College	Yavapai County	

Table 1- Arizona Community and Tribal Colleges

Masters Student recruiting will aggressively target Arizona Military Bases (see Table 2) and Arizona four-year colleges, including the University of Arizona, Arizona State University, and Northern Arizona University.

Base	Primary	Location
Barry M. Goldwater Range	Air Force	Phoenix
Davis-Monthan AFB	Air Force	Tucson
Luke AFB	Air Force	Glendale
Camp Navajo	Army	Flagstaff
Fort Huachuca	Army	Cochise County
Yuma Proving Ground	Army	Yuma County
Marine Corp Air Station (MCAS) Yuma	Marines	Yuma

Table 2 - Arizona Military Bases

U.S. Military personnel who already have an undergraduate degree and who are returning to civilian life will be specifically targeted for recruitment, with annual presentations to be made at all appropriate Arizona military bases. Military personnel from the bases are partners on the Borders and other recent projects; their advice and introduction to the appropriate personnel will be invaluable. Beyond the State of Arizona additional recruiting information will be sent to select U.S. Minority Serving Institutions including Hispanic Serving Institutions located in the Southwest, Historically Black Colleges and Universities (HBCUs) (no geographic limitation, but with the nine HBCUs in Texas being specifically targeted). Such information will be followed up with personal phone calls by the program coordinator and/or participating faculty members, as personal contact can enhance the effectiveness of the mailings.

Ph.D. Student Recruiting will target similar demographics as the Masters Student recruiting; however, Ph.D. funding covers the final three years of research-based doctoral-level study. As the Ph.D. program in the MIS department is a four-year program, in the first year of our program, current Ph.D. students meeting the eligibility requirements will be recruited. We will also recruit students seeking to enter the Ph.D. program who will be suitable for recruitment after their first year of study.

To apply, students will complete an application form and, if found to be eligible for the program, will be subject to an interview.

B. Student Eligibility, Selection Process, and Criteria

The initial pool of applications will be reviewed for program eligibility specifically including eligibility to work for the federal government. Eligibility will be based on citizenship, academics, course of study, and eligibility requirements. For all undergraduate students, citizenship verification will be coordinated through the undergraduate office, which maintains and/or has access to all necessary student information to make this determination. At the graduate level, citizenship information will be provided by the Graduate Admissions Coordinator and financial need status will be provided by the departmental Business Manager and the University Financial Aid office.

Criteria	Ranking Basis
Eligibility	US Citizenship, OPM Approval
Academic Merit	Grade Point Average(s), Transcripts, Recommendations
Communication Skills	Written Work, Interview
Interest in Cybersecurity or Information Assurance	Interview, Prior Academic Work, Professional Experience
Commitment	Interview, Prior Academic Work, Professional Experience

Table 4 – Criteria for Judging SFS Applicants

In addition to meeting the Department's standards for admission, students who are accepted into the program will be also be required to proactively commit to the appropriate course of study, a federal internship, and at least two years of federal service upon graduation. Applicants will be asked to sign a Memorandum of Agreement which attests to their understanding of and willingness to fulfill these obligations.

Student applications will be reviewed and ranked by a committee comprising the PI and Co-PIs. The criteria for judging applicants will specifically include eligibility, academic merit, capability, and commitment to fulfilling all program requirements (see Table 4).

The committee will formalize a weighted decision table to ensure a consistent and evenhanded treatment of all student applicants. This table will be based on these areas and may add additional judging criteria as appropriate and consistent with the SFS program.

All applicants selected for scholarships will have a final interview and fact check to ensure the integrity of the application. Applicants selected for scholarships will be submitted to the OPM for final verification of eligibility before any award is made. Ongoing eligibility and progress assessment will also be confirmed for all renewal applications.

C. Scholarship Awards

Awards will be based on the Academic Year and will not include internship funding.

	Scholarship Period	Annual Stipend	Annual Health Insurance	Annual Prof. Development	Annual Books Allowance
Undergraduates	2 years	$20,000	$1,200	$1,300	$1,000

Masters students*	1.5 years	$25,000	$1,200	$1,300	$1,000
Ph.D. Students	3 years	$30,000	$1,200	$1,300	$1,000

***** Note: The stipends for Masters students will be prorated for the program duration, which is 1.5 years.

Table 3 – Scholarship Awards

D. Student Mentoring and Development (including Independent Study)

All students will be assigned to a dedicated faculty mentor (see Table 5) who will also serve as their research advisor for their required Independent Study in an area relevant to Information Security. Mentors will be assigned based on a shared research interest with the student. Students will be required to participate in research activities (e.g., in one of the faculty labs, or with a new or ongoing research project under the direction of the faculty) for the duration of their tenure at the University by taking an independent study course or dissertation credits every semester. The expected time commitment is two credits per semester (6 hours per week) for undergraduates and masters students, and three to nine credit hours (9 to 15 hours per week) for Ph.D. students. For this effort, they will receive Independent Study credits each semester. This research effort will specifically include work towards an undergraduate thesis for Undergraduate Students, a Master's thesis for all Masters Students and a Dissertation for all Ph.D. Students. Students will meet with their mentor regularly to assess and support both their ongoing research and their normal course of study. Grade checks will be conducted during each semester as part of the program management and the student's faculty mentors will be made aware of any necessary corrections to ensure successful outcomes.

Graduate students will be required to complete their Master's Thesis or PhD Dissertation on an appropriate security topic, to be approved by the PI and their faculty mentor. Masters students will be required to present their Masters Theses to the security cohort for discussion and dissemination. Ph.D. students will be required to publish their research in a peer-reviewed journal publication. All awardees will be required to work with their faculty mentor in addition to the cohort mentor to ensure suitable government internships or research assignments (Ph.D. Students only, with approval of the NSF program office) between their first and second year. Additional faculty will be recruited to serve as student mentors as needed.

Faculty Member	Department
Dr. Hsinchun Chen	Management Information Systems
Dr. Jay Nunamaker	Management Information Systems
Dr. Paulo Goes	Management Information Systems
Dr. Mark Patton	Management Information Systems
Dr. Salim Hariri	Electrical and Computer Engineering
Dr. Christian Collberg	Computer Science
Dr. Saumya Debray	Computer Science
Dr. Matthew Hashim	Management Information Systems
Dr. Joe Valacich	Management Information Systems

Table 5 – Faculty Mentors

In addition students will engage in ongoing development activities outside the classroom as well as through the traditional learning environment. This will include participation in SFS conferences and seminars every semester. During the academic-terms Students will participate in bi-monthly events hosted at the University of Arizona that include seminars on cutting-edge security research, emerging security challenges, and the latest developments in security practice.

Activities will combine a focus on Information Security with a casual, social atmosphere. Examples of activities proposed include a lunch and a speaker, or a tour of relevant companies and other organizations, and a discussion. This will be modeled on the MIS department's very successful program for freshmen and sophomore students focused on MIS in general, which includes such activities as a baseball game followed by a tour of the server rooms and a discussion of the information systems and knowledge used in sports. The project team will also leverage its considerable ties to the local business community (e.g., through MIS

Advisory Board members) to engage speakers and elicit tours of business and industries to showcase their successful information systems and information security methods. These educationally relevant events will also serve to build a sense of community among the cohorts and thus reinforce student retention.

In addition to the individually assigned faculty research mentor, the SFS scholarship cohort will have a dedicated cohort mentor who will manage an ongoing student support program to build a sense of community and provide ongoing support through graduation and employment. The keystone of these programs will be the Program Administrator, who will also fulfill the cohort mentor role, and who will arrange for bi-monthly activities that bring the cohort together outside the classroom to foster community, as well as coordinating attendance at SFS seminars, conferences, and events. In addition, the department provides support for all MIS students through the MIS Department's Career Development Program Coordinator and the Department's Masters MIS Graduate Coordinator. The faculty cohort mentor will work with these existing resources and be administratively supported by a program coordinator.

1. Coursework and Enterprise Security Certificate

The University of Arizona department of MIS is an elite program, currently ranked #3 in the nation for undergraduate education and ranked in the top five MIS programs in the country (*U.S. News and World Report*) consistently for over 20 years, an achievement matched only by MIT and Carnegie-Mellon. The Eller College is fully accredited by the AACSB. In addition to completing their MIS coursework and receiving the Bachelor's, Master's, or Ph.D. degree, each student in the program will be required to earn an Enterprise Security Certification.

The MIS department has been designated by the National Security Agency (NSA) and the Department of Homeland Security as a Center of Academic Excellence in Information Assurance Education (CAE-IAE). In line with this designation, the department has developed graduate and undergraduate courses that students take to receive the National Security Agency's (NSA) Committee on National Security Systems (CNSS) certificates including:

- CNSS 4011 – Information Systems Security Professionals
- CNSS 4012 – Senior Systems Managers
- CNSS 4016 – Risk Analyst
- CNSS 4013 – Systems Administration

These certificates are available through a set of three undergraduate courses, through a set of three graduate courses, or via online graduate courses. Taking either the three online or the three classroom graduate courses will entitle students to also receive an "Enterprise Security Certificate" from the University of Arizona. The options for the Enterprise security certificate are shown in Table 6.

Course Title	Required / Elective
Information Security in the Public and Private Sectors	Required Core Course
Information Security, Risk Mgmt., Disaster Recovery	Required Core Course
Introduction to Enterprise Computing Environments	Elective (1 required)
Systems Security Management	Elective (1 required)

Table 6 – Enterprise Security Certificate Course Options

2. Core Departmental Security Courses – Detail

Information Security in Public and Private Sectors
This course exposes the student to a broad range of computer systems and information security topics. It is designed to provide a general knowledge of measures to ensure confidentiality, availability, and integrity of information systems. Topics range from hardware, software and network security to INFOSEC, OPSEC and NSTISS overviews. Components include national policy, threats, countermeasures, and risk management among others. Course topics include:

- Information Assurance, NSTISS and InfoSec overview

- Legal Elements of Information Security
- Information Security Governance
- Security and Personnel
- Automated Information Systems and Operating Environments
- Security Planning
- Security Auditing and Monitoring
- Network and Operations Security
- Physical and Infrastructure Security
- Identification, Authentication, and Access Control

CNSS Certificates: CNSS 4011 – Information Systems Security Professionals
CNSS 4012 – Senior Systems Managers

Information Security, Risk Management, Disaster Recovery
This course examines the principles of computer and information security, information assurance (IA), the range of cyberthreats to organizations, TVA (threat-vulnerability analysis), IA risk management strategies, Info security countermeasures and business contingency planning. A team-based “Info Security Assessment” project is required for analysis, presentation and course certification. Course topics include:

- Introduction to Computer and Information System Security
- Cyber-Threats (internal and external)
- Adversary Analysis (*cyber-attack methods*)
- Threat Vulnerability Analysis (*TVA*)
- Risk Management - Identification and Assessment
- Risk Management Strategies (Avoidance, Transference, Mitigation, Acceptance)
- Risk Management - Counter-Measures, Cyber Warfare (*Technical and People*)
- Vulnerability Testing and Penetration Testing
- Contingency Planning (Business Impact Analysis, Disaster Recover, Business Continuity)
- SETA*:* Security, Education, Training and Awareness Initiatives
- Cost Benefit Analysis of Info Security investments

CNSS Certificate: CNSS 4016 – Risk Analyst

Systems Security Management
The information security arena contains a broad array of multi-level models for assessing, planning, implementing, monitoring and mitigation of security risks. At the very core of this information security spectrum are the actual system and network devices which store, manage, transmit and secure information. This course is designed to provide a working knowledge of issues and techniques surrounding the proper safeguarding of operating systems and related components. Filled with Information Assurance topics, this course offers a solid base for system administrators and technical managers. Course topics include:

- CNSS & Security Basics
- Operational Security
- Operating System Security
- Authentication & Encryption
- Account-based Security
- Firewalls & Border Security
- Email Security
- Disaster Recovery, Business Continuity, & Incident Response
- Auditing & Monitoring

CNSS Certificate: CNSS 4013 - System Administrators

E. Assessment of Student Progress

Students will be required to submit their course schedule at the start of each semester to the program administrator, and their grades at the end of each semester. To encourage academic performance, all students participating in the program will be required to maintain a 3.0 GPA overall and receive a minimum of a B in all security certificate courses. The program administrator will also maintain documentation on student participation in events and on completion of other required activities, such as internships and research progress. Performance and eligibility will be reviewed on a semester-by-semester basis, with the program administrator also consulting with the faculty advisors for scheduled thesis and dissertation reviews to ensure ongoing and appropriate progress. Students will be provided with appropriate feedback and recommendations if they need to make adjustments to their performance or activities in order to remain in the program. If a student in a program loses eligibility for a semester and then returns to good standing, he or she may apply to be reinstated. Our objective is for all students admitted to the program to successfully complete the program and their degree.

F. Data Management Plan

Completed Theses and Dissertations will be submitted to the University of Arizona library and to the ProQuest – UMI Dissertation Publishing service for archiving and accessibility to a broader audience. All NSF SFS student records will be kept in a locked file cabinet in the program administrator's office. Scholarships will be deposited into the students Bursars account by the business manager each semester upon approval of the course of study.

G. Internships and Post-Graduation Placements

All Undergraduate and Master's Students will be required to apply for and secure government internships between their first and second years, and that all students apply for and secure a government position upon graduation.

The program administrator will be responsible for coordinating student interaction with the OPM and facilitating the utilization of OPM services for internship and job placement. These activities will primarily leverage and be coordinated with the already significant levels of support provided all MIS students by the MIS Department's full-time Career Development Program Coordinator and the Department's Masters MIS Graduate Coordinator.

H. Program Assessment and Evaluation

Assessment and evaluation will be both quantitative and qualitative. Students will be surveyed when entering the program and at the end of each semester on courses taken, planned enrollments, deviations from approved study plans, progress towards cybersecurity certifications, research performed, research interests, faculty mentor interactions, program administration and execution, and on cohort activity metrics. In addition, student academic performance and course completion will be evaluated.

Faculty mentors will also be surveyed at the end of each semester on faculty mentor interaction, student research performance, student engagement, and program administration and execution. An external evaluator will execute the surveys, compile metrics, conduct follow-up interviews with select students and faculty, report on the program status and make recommendations for ongoing improvements to both the program and the Evaluation Plan. This will include metrics regarding recruitment, retention, satisfaction, and graduation rates will be evaluated against program targets. Performance, targets, and variances will be reviewed every semester for cause and necessary adjustments to ensure program success.

A terminal assessment by an external evaluator will be conducted to highlight things done right, opportunities for future growth, overall program success, and adjustments necessary going forward to ensure the program accomplishments continue on a self-sustaining basis. Specific metrics to be reviewed will include the impact of scholarships on recruitment, retention, and growth. We will also review policies on student performance and their impacts on retention and student outcomes. Finally, we will look at student support programs and their impacts, and conduct interviews with students after initial placement.

III. Program Management and Project Personnel

I. Management Structure Overview

The program will be under the direction of the PI and advised by the co-PIs on program performance and direction. The program will be managed on a day-by-day basis by Mark Patton, PhD. Mark will be designated as the SFS Program Administrator and cohort mentor. The overall organizational structure is depicted in Figure 1.

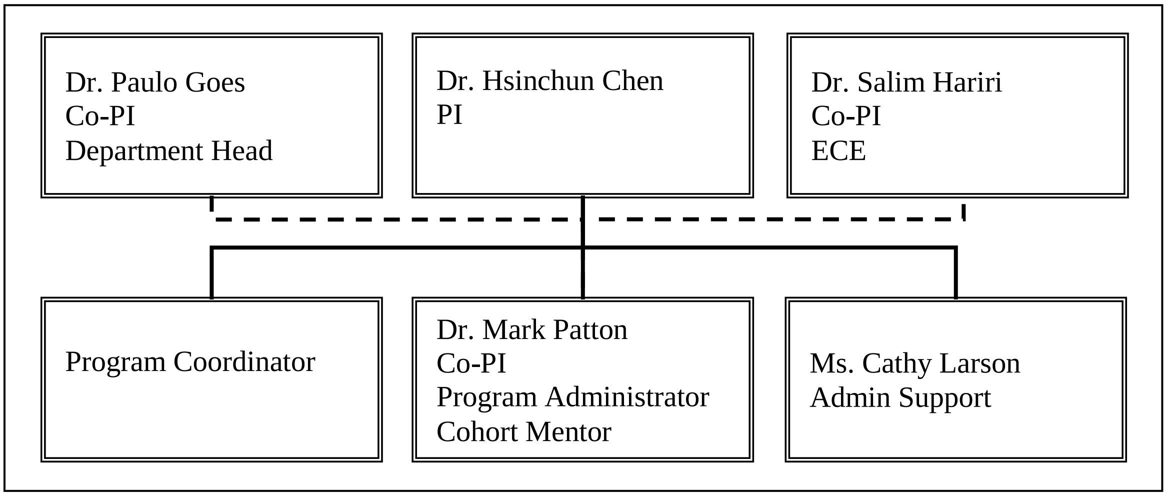

Figure 1 – Organizational Structure

J. Project Personnel

Dr. Hsinchun Chen will serve as project PI. He is the McClelland Professor of Management Information Systems at the University of Arizona. Dr. Chen actively teaches in the MIS department, has conducted extensive research in security informatics for a number of years, is the Director of the Artificial Intelligence Lab, and, as described in the section on Department Research has an extensive track record of successfully managing NSF grants. He received the B.S. degree from the National Chiao-Tung University in Taiwan, the MBA degree from SUNY Buffalo, and the Ph.D. degree in Information Systems from New York University. Dr. Chen has served as a Scientific Counselor/Advisor of the National Library of Medicine (USA), Academia Sinica (Taiwan), and National Library of China (China). He is also a Fellow of IEEE and AAAS, and received the IEEE Computer Society 2006 Technical Achievement Award and the INFORMS Design Science Award in 2008. He is the author/editor of 20 books, 25 book chapters, 200 SCI journal articles, and 130+ refereed conference articles covering Web computing, search engines, digital library, intelligence analysis, biomedical informatics, data/text/web mining, and knowledge management.

Dr. Paulo Goes, MIS Department Head and Salter Distinguished Professor in Technology and Management, will serve as Co-PI and brings great depth to the information security program. As the department head of MIS, he will participate in recruitment efforts as well as the special events planned for the student cohorts. His areas of expertise include Information technology evaluation, electronic markets, database security and confidentiality protection, technology infrastructure, and network design and performance. He received his Ph.D. from the William E. Simon Graduate School of Business Administration University of Rochester in Computers and Information Systems. Prior to coming to the University of Arizona, he was Gladstein Professor of Information Technology and Innovation, Operations and Information Management, at the School of Business, University of Connecticut.

Dr. Salim Hariri, Professor in the Department of Electrical and Computer Engineering, is Co-PI and also brings great exceptional research programs in which students can gain relevant, timely experience highly pertinent to their studies as well as future professional or academic positions. He teaches Cybersecurity (ECE 509) and has developed an Industrial Cybersecurity test-bed as well as a network security testbed that can be leveraged for student research. As described above, Dr. Hariri has significant federal research support for cybersecurity and his team has transitioned the technologies supported by ARL and the Air Force into commercial products and received STTR and SBIR funding.

Other faculty from MIS, Electrical and Computer Engineering, and Computer Science have expressed enthusiasm for serving as mentors to enrolled students (Table 5, above). These are faculty who, as research partners, have brought a special depth and synergy to collaborative projects and who are also recognized as excellent teachers and mentors. Their contribution will include mentoring student research projects for the Independent Studies and participating in program events as speakers and presenters.

Dr. Mark Patton is a Lecturer in MIS and Director of the Hoffman E-Commerce Laboratory and will serve as Co-PI in the roles of Program Administrator and cohort mentor. He teaches both undergraduates and graduate students in the MIS Department. His research interests include decision support systems for automated deception identification, HCI with embodied conversational agents, organizational modeling and simulation, and agent based systems. The Hoffman E-Commerce Lab provides instructional and research support with a focus on providing access to high-end hardware and software technology and facilitating collaborative projects between the University and private industry. Dr. Patton earned the Ph.D. in Management Information Systems from the University of Arizona in 2009. As program administrator and cohort mentor, he will provide significant day-to-day mentoring and oversight of students in the program.

As cohort mentor, primary responsibilities will include development and oversight of recruitment activities, overseeing the selection process, ongoing management, and arranging special events. Mentor responsibilities will include special office hours weekly reserved for both graduate and undergraduate SFS students and meeting with the students individually and as a group bi-monthly, tracking each student’s individual progress. The cohort mentor will work closely with and be supported in program implementation by a program coordinator, and will be responsible for ensuring that Undergraduate and Master’s Students apply for and secure government internships between their first and second years along with ensuring all students apply for and secure a government position upon graduation. During the academic year, the cohort mentor will maintain communications with faculty mentors, engage them as presenters and participants, and match student needs and interests with those of interested faculty mentors. Reports will be provided every semester to the PI indicating student progress and continued eligibility. The cohort mentor will work with the program coordinator to provide reports and maintain documentation on internship placement and government position placement for graduates and coordinate student interaction with the OPM, facilitating the utilization of OPM services for job placement. These activities will be coordinated with and leverage the already significant levels of support provided all MIS students by the MIS Department’s admissions personnel, full-time Career Development Program Coordinator and the Department’s Masters MIS Graduate Coordinator.

The program coordinator (TBD) will set-up and carry out in-person recruiting events and visits as designed by Dr. Patton, as well as follow-up activities, and will support ongoing program management activities. He or she will also schedule, arrange, coordinate, and manage publicity and invitations for all seminars and other events for the SFS students, as well as schedule and arrange the events themselves.

Ms. Catherine A. Larson is Associate Director of the Artificial Intelligence Lab, a position she has held since 2003. She earned the MSLIS from the University of Illinois in 1980. Ms. Larson has significant experience in coordinating information systems projects and programs. Her responsibilities will include working with Dr. Patton in matching interested students to AI Lab internship opportunities, assisting the external consultant with assessment, and providing additional administrative support and financial management and reporting.

K. Management Plan Timeline

The NSF SFS program will go into effect starting with the 2013-2014 academic year. Recruitment will begin immediately upon approval to capture students during the 2012-2013 academic years. The timeline, shown in Table 4, will repeat annually, with applicants applying for renewal submitting their renewal applications at the same time as new applicants.

	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug
Recruiting and Admissions Activities													
Recruiting and Awareness	Graduate	Graduate	Graduate	Graduate				Undergraduate	Undergraduate	Undergraduate	Undergraduate		
Application Submission		Graduate	Graduate	Graduate					Undergraduate	Undergraduate	Undergraduate		
Application Review					Grad.						Undergrad.	Undergrad.	
Scholarships awarded						Grad.						Undergrad.	Undergrad.
Kickoff & Welcome													All
Plans of Study / Research Approved													All
Funds Disbursed						All							All
Ongoing Activities and Research													
Tour / Speaker			All		All		All		All				
Summer Internships										All	All	All	All
Regular Research & Study	All	All	All	All	All	All	All	All	All	All			
Approved PhD Summer Research										PhD	PhD	PhD	PhD
Study & Research Assessments						All				All			All
Graduations					All					All			

Table 4 – Timelines

The initial pool of scholarships will be awarded as soon as possible, although students won't actually receive the funds until they are committed, in attendance, and have an approved schedule. Funds will be deposited in Bursars accounts prior to the late payment deadline to avoid making the students borrow excess funds. There will be a kick-off event for all scholar recipients to start forming community bonds during the first week of school.

Once the program is up and running, there will be events or tours approximately every two months, specifically in October, early December (will also serve as a sendoff for December graduates), late February, April, and a sendoff event for graduating students in early May. Combined with the annual August kick-off, this will result in six formal student support events a year. Students will be expected to attend as many as possible, at least four, although reasonable accommodations will be made for students who have restrictions. There will be academic checks during and at the end of each semester, individual mentoring meetings with the cohort mentor, thesis and dissertation reviews, ongoing engagement with faculty mentors, and meetings to ensure students apply for and secure federal internships and federal employment upon graduation.

IV. Significance of Project and Rationale

The MIS department has recently determined that Information Security will be one of its three "pillars of excellence." This was decided based on our growing body of offerings and, as described in the Introduction, on the steadily growing demand in the job market for security professionals and/or professionals with a security background, and our ability to consistently remain ranked within the top 5 schools for the last twenty years. Based on this, implementing a Scholarship-for-Service program targeting Arizona minorities and former military personnel was a logical next step to strengthen the program, provide service to Arizona, and to support the ongoing cybersecurity and Information Assurance needs of federal agencies.

Currently the undergraduate program has 114 enrollments for the 2011 academic-year. The cybersecurity courses are especially popular, with 52 students registered for "Information Security, Risk Management, and Disaster Recovery." However, a smaller segment of the undergraduate population targets cybersecurity as their primary career focus, and many of them are targeting careers in the private sector. Strengenthening the program will help meet the steadily growing demand for information security professionals (Foote & Reynolds, 2009).

At the graduate level, the MIS program is also very strong, with 90 Masters and 9 Ph.D. students entering the program for the 2011 academic year. Again, there is strong interest in the security classes at the graduate level, with students are split between information assurance, business intelligence, and other MIS focus areas as their primary area of study. Recruiting key students who are both interested in and eligible for government service after graduation will again both strengthen the program and support the growing need for security professionals suitable and qualified for federal government employment.

Currently the department does extremely well with retention, with 96% of MIS declared undergraduates graduating from the University of Arizona with an MIS degree, and 99% of declared MIS masters students graduating from the University of Arizona with an MIS Master's degree. Retention really is not the problem, so much as recruitment to service work force demand.

V. Activities on Which the Current Project Builds

L. Zipperman Scholars program for Undergraduate Students

The current project will build on current student support elements. At the undergraduate level, the department has a scholarship program for a large cohort of freshmen and sophomores who are being recruited to pursue MIS as a career. The program had 112 freshmen and sophomore participants in the Spring 2012 academic semester.

This program, funded by Walt Zipperman, is the Zipperman Scholars program, and it attracts a diverse mix of students who participate in many activities such as tours and seminars. There is a pool of underrepresented undergraduate students within this program who have a solid educational background and who would be highly suitable for the SFS scholarship program. These students will be targeted for recruitment into the SFS scholarship program, and the model of activities and seminars will be emulated for the SFS security cohorts, while also being expanded to include appropriate SFS events, conferences, and seminars.

M. Departmental Research, Research Dissemination, and Outreach

The MIS and ECE departments each have had long and unique involvement with Information Security, Security Informatics, information assurance, and many related domains.

Dr. Chen, the PI for this proposal, heads up the Artificial Intelligence Lab (http://ai.arizona.edu/), which originated the COPLINK software now used nationwide by police agencies to manage and utilize their data (Wang et al., 2004; Hu et al., 2005; Kaza et al., 2009). The AI Lab, established over 20 years ago, is generally staffed with 10-15 graduate, Ph.D., and undergraduate students at any one time, all of whom carry primary responsibilities for all phases of research projects. Dr. Chen also founded the IEEE Intelligence and Security Informatics conferences (http://www.isiconference.org/), the premiere international conference for security informatics research. Dr. Hsinchun Chen, with colleagues Dr. Daniel Zeng and Dr. Feiyue Wang, founded this annual conference with the sponsorship of the National Science Foundation and other agencies; it is now held under the auspices of the IEEE Society. Its first two meetings were held in Tucson, Arizona in 2003 and 2004. With generous "start-up" funding from the Department of Justice, CIA, NSF, and the DHS, the meetings attracted and continues to attract a global ICT audience of researchers, academicians, practitioners, and representatives from government agencies who care about various security-related research topics. The conferences have continued annually in a variety of U.S. and international locations; additional spin-off conferences have also been held such as the Pacific-Asia ISI Workshop and the European ISI Workshop, both of which are hosted by a new location each year. Security informatics research has truly become an international research agenda, and the conferences continue to attract academic researchers, practitioners, and representatives from government agencies.

Much of Dr. Chen's present research focuses on analyzing the "Dark Web," described above, which examines social media participants linked through their affinity with or sponsorship by terrorist organizations (Zimbra et al., 2010; Xu and Chen, 2008). In a related project, Dr. Chen's research group is experimenting with various multilingual data mining, text mining, and web mining techniques as well as content and sentiment analysis, authorship analysis, and video analysis to study country risk more broadly. Dr. Jay Nunamaker, the founder of the MIS department at the University of Arizona, continues to actively pursue relevant research and is an active collaborator with Dr. Chen and others in the department. Dr. Nunamaker is the head of the DHS-funded National Center for Border Security and Immigration (BORDERS) research center (http://www.borders.arizona.edu/). Both are U.S. citizens and hold security clearances.

Dr. Salim Hariri, ECE department, is most recently working on 1) “Moving Target Defense Middleware (MTDM) for Intrusion Resilient Cloud Services,” (supported by grants from the Air Force Office of Scientific Research (AFOSR), AVIRTEK, and NSF Cloud and Autonomic Computing Center), and 2) “Anomaly Behavior Analysis (ABA) of Communication Protocols” (supported by grants from the Army Research Laboratory, the Air Force Research Lab, Raytheon, AVIRTEK, and NSF Cloud and Autonomic Computing Center). In 1), Dr. Hariri’s team is developing a new approach to cybersecurity. The novel capabilities of their MTDM include tolerating a wide range of malicious cyber attacks, delivering uninterrupted cyber-enabled services and applications in spite of persistent attacks, and effecting a MTD designed to shift the advantage to defenders over attackers. In 2), the main goal is to investigate innovative anomaly behavior analysis methodology that is significantly different from current practices and can overcome the inherent limitations, particularly the high false-alarm rate. The team will investigate the use of specialized anomaly detection algorithms that focus on analyzing the behavior of communication protocols, services and hardware resources and then fuse their results to significantly improve the accuracy and reduce the false alarms. This approach has been successfully demonstrated to detect network and application attacks with high detection rates and low false alarms. Dr. Hariri's recent proposal to AFOSR, "DDDAS-based Resilient Cyberspace (DRCS)," about applying autonomic computing and moving target defense strategy to make cloud systems and services resilient to attacks, will provide another interesting avenue for student involvement in research relevant to real-world problems.

Other faculty from MIS, Electrical and Computer Engineering, and Computer Science have expressed enthusiasm for serving as mentors to enrolled students (Table 5). These are faculty who, as research partners, have brought a special depth and synergy to collaborative projects and who are also recognized as excellent teachers and mentors. Their contribution will include mentoring students’ Independent Research projects and participating in program events as speakers and presenters.

VI. Dissemination

Dissemination to peer institutions will occur through journal articles and academic conferences. The IEEE Intelligence and Security Informatics (ISI) conference (described above) in particular will be targeted for dissemination on the program outcomes and effects on growing and strengthening our Information Security program. This conference and its Asian and European counterparts has had nearly 1,000 participants over the years, and attracts academic researchers as well as practitioners.

Graduate thesis work will be disseminated through publication with ProQuest – UMI Dissertation Publishing as well as through presentations at appropriate conferences and seminars. Project outcomes and the measurements used to assess them may be of particular interest to education researchers. That audience will be targeted through education journals, such as *Educational Research and Evaluation, IEEE Transactions on Education*, and *The Review of Higher Education.*

VII. Summary

Since pioneering one of the nation's first Management Information Systems (MIS) curriculums three decades ago, the Eller College of Management MIS Department at The University of Arizona has become a leader in IT education and research. By leveraging the University’s unique research and teaching strengths in information systems, Security Informatics, and information security coursework and certificate program, we believe this proposed NSF SFS program will allow us to graduate students who are well prepared to face the daunting security challenges facing IT progress generally and governmental information systems specifically.

VIII. Results from PI's Prior NSF Support (selected)

As mentioned in the Introduction, the PI has extensive experience managing successful information systems and intelligence and security informatics research and has received over $30 million in funding through grants, awards and contracts from National Science Foundation, National Institutes of Health, and various government agencies. Below are three selected programs which best represent the PI's mastery of relevant security-related subject knowledge and ability to successfully carry out the proposed program. In all cases, the programs described here had (or still have) significant partnership funding in addition to the funding provided by NSF. In each case, the results are followed by a description of the funding and, owing to space constraints, citations to two selected papers only. Additional relevant citations may be found at ai.arizona.edu.

N. COPLINK Center for Homeland Security Research (NSF-Digital Government/DHS/CIA, 2000-2007, $3.1M):

Principal investigator of a major NSF Digital Government project for developing information sharing and criminal analysis technologies for law enforcement and homeland security community, and founder/developer of COPLINK, cross-jurisdictional information sharing, analysis, and visualization software for the law enforcement and intelligence communities. The COPLINK system has been adopted in more than 4,600 agencies in the U.S. The COPLINK research received "The PTI Technology Award" in the public safety category for mid-size cities in 2003 and has been featured in numerous law enforcement publications and general news media. In addition to greatly improving the public safety agencies' information management capabilities, the COPLINK Center had an important role in furthering homeland security and counter-terrorism research in the areas of data mining, visual analytics, and knowledge management. In the summer of 2009, COPLINK was acquired by i2 for integration with its popular i2 crime analysis and visualization toolkit, the Analyst Notebook; i2 was acquired by IBM in July 2011, making COPLINK one of the most financially and programmatically successful UA start-ups in the university's history.

NSF Funding: 1) Principal Investigator (PI), NSF, Digital Government Program, "COPLINK Center: Social Network Analysis and Identity Deception Detection for Law Enforcement and Homeland Security," $600,000 (IIS-0429364), September 2003-August 2009. (UA matching: $75,000). 2) Principal Investigator (PI, Co-PI: D. Zeng), NSF, Information Technology Research (ITR) Program, "COPLINK Center for Intelligence and Security Informatics--A Crime Data Mining Approach to Developing Border Safe Research," $700,000 (EIA-0326348), September 2003-August 2009. (UA matching: $175,000)

Two Selected Papers: 1) D. Hu, S. Kaza, and H. Chen, "Identifying Significant Facilitators of Dark Network Evolution," *Journal of the American Society for Information Science and Technology*, 60:4, pgs. 655-665, April 2009. 2) S. Kaza, J. Xu, B. Marshall, and H. Chen, "Topological Analysis of Criminal Activity Networks: Enhancing Transportation Security," *IEEE Transactions on Intelligent Transformation Systems*, 10:1, March 2009.

O. A National Center of Excellence for Infectious Disease Informatics (NSF/ITR, 2004-2010, $2.2M):

Principal investigator for a collaborative initiative (BioPortal) to explore the development of an integrated and scalable information sharing, monitoring and analysis environment across jurisdictions and for different infectious diseases (e.g., west Nile virus, foot-and-mouth disease). BioPortal has become one of the major infectious disease tracking systems in the US. Research Experience for Undergraduates (REU) supplemental funding has also been awarded for this work, allowing us to integrate highly motivated undergraduates into our research processes.

NSF Funding: Principal Investigator (Co-PI: D. Zeng), NSF, Information Technology Research (ITR)

Program, "A National Center of Excellence for Infectious Disease Informatics," $1,200,000 (IIS-0428241), August 2004-July 2010. (subcontracts and partners: University of Utah, California Department of Health, and NY Department of Public Health) (UA matching: $75,000)

Two Selected Papers: 1) H. Lu, D. Zeng, and H. Chen, "Prospective Infectious Disease Outbreak Detection Using Markov Switching Models," *IEEE Transactions on Knowledge and Data Engineering*, 22:4, pgs. 565 - 577, April 2010. 2) Y. Dang, Y. Zhang, H. Chen, P. Hu, S. Brown and C. Larson, "Arizona Literature Mapper: An Integrated Approach to Monitor and Analyze Global Bioterrorism Research Literature," *Journal of the American Society for Information Science and Technology*, 60:7, pgs. 1466-1485, July 2009.

P. Dark Web Research Program (NSF, 2007-2010, $1.5M):

Principal investigator of several NSF projects that aim to develop computational approaches to understanding global extremism and terrorism phenomena on the Internet. The AI Lab’s Dark Web project is a long-term scientific research program that aims to study and understand the international terrorism phenomena via a computational, data-centric approach. A primary goal is to comprehensively collect web content generated by international terrorist groups, including web sites, forums, chat rooms, blogs, social networking sites, videos, virtual world, etc. We have developed various multilingual data mining, text mining, and web mining techniques to perform link analysis, content analysis, web metrics (technical sophistication) analysis, sentiment analysis, authorship analysis, and video analysis in our research. The approaches and methods developed in this project contribute to advancing the field of Intelligence and Security Informatics (ISI). Such advances help related stakeholders to perform terrorism research and facilitate international security.

NSF Funding: 1) Principal investigator, NSF, "CRI: Developing a Dark Web Collection and Infrastructure for Computational and Social Sciences," $500,000 (CNS-0709338), October 2007-September 2010. 2) Principal investigator, NSF, "EXP-LA: Explosives and IEDs in the Dark Web: Discovery, Categorization, and Analysis," $800,000 (CBET-0730908), December 2007-November 2010.

Two Selected Papers. 1) H. Chen, W. Chung, J. Qin, E. Reid, M. Sageman, and G. Weinmann, "Uncovering the Dark Web: A Case Study of Jihad on the Web," *Journal of the American Society for Information Science and Technology*, 59:8, pgs. 1347-1359, 2008. 2) Abbasi, A., Chen, H. and Salem A., "Sentiment Analysis in Multiple Languages: Feature Selection for Opinion Classification in Web Forums," *ACM Transactions on Information Systems*, 26:3, Article 12, June 2008.