Scholarship for Service (SFS) PhD with Information Assurance (IA) Concentration*

University of North Texas (UNT) received a NSF award to provide scholarships, including stipends, tuition, health insurance, travel and textbooks, to enable **US citizens** to pursue a PhD degree in information assurance (IA) on a full-time basis. The University of North Texas Interdisciplinary Information Assurance PhD Program responds to the varied and changing needs of an information age. This program's graduates will be prepared to contribute to the advancement and evolution of the information society in a variety of roles and settings as scientists, educators, administrators, and information security architects.

Here are the program's features*:

Students receive admission to a PhD program in one of home departments below and meet all department requirements.

Computer Science and Computer Engineering (CSE)

- Students are enrolled in CSCE in a 4-year PhD program (72 credits) after BS or (42 credits) after MS.

Information Technology and Decision Sciences (ITDS)

- Students are enrolled in ITDS in a 4-year PhD program (60 credits) after Masters

Library and Information Sciences (LIS)

- Students are enrolled in Information Sciences in a 4-year PhD program (60 credits) after Masters

Information Assurance Concentration

- Students will be selected for the SFS award after the first year (completing core and electives) and sign the agreement with US Office of Personnel Management (OPM) and begin receiving SFS funding
- Students must participate in a monthly doctoral colloquium of speakers and activities,
- Students receive all the security certificates offered in UNT (e.g., 4011, 4012 and 4013, see cics.unt.edu for details)
- Students must meet the requirements to receive the summer research-intern opportunities provided by federal, state and local agencies (with the help of advisory board and OPM.)
- SFS students receive a $30K/nine-months stipend. As summer research/interns, students will receive a salary from their host organization for three months (salary varies based on the host organization). SFS students receive tuition scholarships of $8.1K/year. In addition, students will be supported $4K/year for the travel, $1.2K/year for books, and $1.5K/year for health insurance.
- With prior permission, students can substitute an internship with a summer-research program in a state university. For example, summer research opportunities are available through the Center for Information and Computer Security, Texas Center for Digital Knowledge, and Center for Decision and Information Technologies (CDIT),

Table 1: Support for SFS students

	Year1	Year2	Year3	Year4	Year5	Year6
Cohort1 (2 students)	**UNT support**	**SFS Year1 Support**	**SFS Year2 Support**	**SFS Year3 Support**		
Cohort2 (2 students)		**UNT Support**	**SFS Year1 Support**	**SFS Year2 Support**	**SFS Year3 Support**	

**Subject to changes based on the discussion/approval in the department and grad school*

Cohort3 (2 students)			**UNT Support**	**SFS Year1 Support**	**SFS Year2 Support**	**SFS Year3 Support**

Note: Major Professors or the home department are responsible for the financial support during a student's first year (through RA, TA and GAT scholarships). The SFS program supports SFS students during their remaining three years. After the end of four years, students should seek employment in federal, state, and local governments. SFS students may substitute research in a state university for Summer Research Internships. In these instances, the major professor will provide or arrange for the summer support.

Timeline:

- Nov 1: Students are encouraged to apply to the PhD program of their choice and through which they are seeking their first year University funding (not SFS Funding) and should have their application complete and at the Toulouse Graduate School by this date.
- Fall of Year 1: SFS students begin their PhD course work.
- Feb 1 of Year 1: SFS PhD program determines candidates for the SFS IA concentration
- March 1 of Year1: SFS PhD program announces SFS scholarship winners (two students per year).
- Fall of Year 2: Winners enter SFS program
- Spring of Year 4: SFS candidates graduate.

PhD Admission:

The UNT Toulouse Graduate School provides an ideal environment for supporting faculty, serving students' needs, and for incubating new interdisciplinary degrees. The Graduate School provides university-level leadership and resources essential for developing and sustaining graduate programs, including: i) allocating state-supported graduate assistantships (teaching assistantships, teaching fellowships, and research assistantships), ii) allocating tuition-remission scholarships , iii) awarding university graduate fellowships and other scholarships, iv) coordinating recruitment activities, especially recruitment from underrepresented groups, and iv) assisting in program marketing and communications. The Graduate School is committed to creating and supporting a successful IA PhD program. Regents Professor Victor Prybutok (associate dean of the Graduate School, and senior personnel in the SFS program), will be working with the core SFS faculty on curriculum development and program assessment.

Selection Criteria:

Students can enter the Interdisciplinary Information Assurance PhD Concentration only in the fall semester. Prospective students must apply and be admitted first to UNT's Toulouse Graduate School. If successful, they must apply to be admitted to a doctoral program in one of the supporting departments (see respective department web sites for details). To ensure full processing by all offices, including international admissions (and scholarships if appropriate), applicants must submit all application materials by November 1 of the year preceding the fall semester of initial enrollment. Applicants must meet the Toulouse Graduate School's general admission requirements and the requirements of the Interdisciplinary Information Assurance PhD Program, as follows:

1. be a U.S. Citizen, 2. complete at least a bachelor's degree from a regionally accredited institution (masters for ITDS and SLIS), 3. earn an overall grade point average of 3.5 GPA on their most recent 30 hours of course work (4.0 scale), 4. submit Graduate Record Examination (GRE) or Graduate Management Admission Test (GMAT) scores including verbal, quantitative and analytical writing, 5. supply three recommendations from former professors, employers, or others who can give evidence of the applicant's interest in and aptitude for a research career in information security, 6. provide a Personal Statement of 300–500 words stating: career objectives (This may include doctoral research areas of interest; research, professional or community experiences that demonstrate motivation, commitment and potential for doctoral work); accomplishments (publications, presentations, awards);

communication skills including multilingual proficiency; technology skills; and contributions to diversity of the field, 7. provide a current, complete Curriculum Vita, 8. submit a sample of formal writing (published paper, major term paper, thesis chapter, etc.), and 9. complete a comprehensive interview with the admissions committee.

IA Concentration: Students complete core courses, electives, research courses, and a dissertation (total of 72 credits; this includes 8 organized courses in IA). The IA concentration will appear on the PhD degree. PhD candidates must satisfy the specific requirements of their home department to secure a PhD. Home departments and the graduate school approve all degree plans.

1. Core Courses (four courses, 12 credits)

CSCE 5550 INTRODUCTION TO COMPUTER SECURITY—Presents theory and practice of computer security, stressing security models and assurance; security goals, threats, and vulnerabilities; cryptography; program security; and operating system security issues. Includes basic network security, planning, policies, and risk analysis.

BCIS 5630 INFORMATION TECHNOLOGY SECURITY - Examines technical and managerial issues associated with the design, development and deployment of security of client/server and other computer systems. Topics include theory and practice of computer basic security and privacy, issues associated with security architectures, platform connectivity and networks.

BCIS 5640 ADMINISTRATION AND POLICY IN INFORMATION SECURITY- Investigates the major concepts and techniques used in client-server systems architecture and information security, beginning with a strategic planning process for security. Subjects include security practices, security architecture and models, continuity planning and disaster recovery planning. Multiple hands-on projects include experiments in buffer overflows, virus detections, DoS attacks, and configuring firewalls, intrusion detectors, and honey pots (pre-requisite: programming language such as C++ or Java).

CSCE 5640 SECURED E-COMMERCE—Explores electronic commerce technology, models, and issues, with an emphasis on security issues. Addresses supporting technology such as cryptography, digital signatures, certificates, and public key infrastructure, as well as security-conscious programming-based applications. Stresses interaction between technical issues and business, legal, and ethical issues. Includes a research project.

SLIS 5960 KNOWLEDGE MANAGEMENT TOOLS AND TECHNOLOGIES (if not available, use CSCE 5215 MACHINE LEARNING)—Provides an introduction to knowledge management technologies, knowledge management processes and corresponding technologies, to collaboration tools and technologies, to information and knowledge portals and issues related to privacy and information security, to the practice of using information and collaboration technologies and processes to enhance organizational learning and improve organizational performance, and to evaluation and selection criteria for knowledge management tools and technologies (if the course is not offered, students can substitute with courses on information retrieval and machine intelligence)

2. Electives (minimum of 12 credits and following is a partial list)

CSCE 5380 DATA MINING— Provides an introduction to data mining which includes main data mining tasks, e.g., classification, clustering, association rules, and outlier detection, and some of the latest developments, such as mining spatial data, mobile and web data. Includes multiple hands-on projects with the existing datasets from mobile phones, Facebook, Twitter, web blogs, and other sources data (prerequisite: programming language such as C++ or Java).

CSCE 5350 DATABASE SYSTEMS—Provides an introduction to the design and use of database systems. Topics include data models, database query languages, logical database design, and dependency theory (pre-requisite: programming language such as C++ or Java).

CSCE 5550 INTRODUCTION TO CRYPTOGEAPHY—The aim of this course is to educate graduate students to the fundamentals of cryptography, . Cryptography is the fundamental building block of any computer security solution. This course will introduce various cryptographic algorithms and their applications. The knowledge gained from this course will enable students to apply these cryptographic algorithms in a better way to design secure systems.

CSCE 5933 DESIGN AND ANALYSIS OF TRUSTED SECURE COMPUTING PLATFORM—

Examines threat models—physical attacks, software attacks, side-channel attacks and defense mechanisms such as tamper evidence, tamper resistance, tamper detection and tamper response.

CSCE 5270 COMPUTER-HUMAN INTERFACES—Emphasizes human performance in using computer and information systems. Topics for software psychology include programming languages, operating systems control languages, database query facilities, computer-assisted dialogues, personal computing systems, editors, word processing and terminal usage by non-skilled users.

CSCE 5570 INTRODUCTION TO COMPUTER NETWORKS— Study of problems and limitations associated with interconnecting computers by communication networks. ISO reference model, architecture of circuits, message and packet switching networks, network topology, routing, flow control, capacity assignment, protocols, coding and multiplexing

CJUS 5100 INFORMATION WARFARE, SECURITY AND RISK ANALYSIS—An in-depth examination of information warfare, the management of information security and the analysis of risk within organizational contexts.

CJUS 5120 CYBERCRIME AND DIGITAL FORENSICS—Examines crimes using computers and the Internet as the criminal's primary medium, with practical analyses of evidence.

ITDS 5690 Topic in Information Security Technology **-** Current issues dealing with the security and information assurance issues of information systems and technologies.

SLIS 5960.1 TOPICS IN INFORMATION SECURITY—Examines risk analysis, security and curatorial aspects of Digital Information Resources, and Compliance.

SLIS 6000 SEMINAR IN INFORMATION SCIENCE—Evaluates social and technical issues responsible for the evolution of information science. Considers major problems, trends, and developments. Provides a critical, historical survey of major works and developments in research and practice.

BCIS 6010 Seminar in Business Information Systems and Technologies – Covers one or more special fields in information systems and technologies.

BCIS 6650Seminar in General systems Theory – study of computer information systems in the context of their interaction with the environment in which they operate, including the human decision maker and how the information system is supported or inhibited by the orientation and design of the environment in which operates.

SLIS 6700 SEMINAR IN COMMUNICATION AND USE OF INFORMATION—Explores nature of information as a phenomenon and of the communication processes. Examines conceptual linkage to treatments in various fields with a focus on the role of information and communication in individual, social and institutional behavior.

SLIS 5960.2 DATA ANALYSIS AND KNOWLEDGE DISCOVERY—Focuses on data analysis and data manipulation including techniques for management of large amount of data generated on daily basis. Develops knowledge discovery techniques and methods and their application to health, social and security information.

BUSI 6220 APPLIED REGRESSION ANALYSIS—Examines Applied Regression Analysis Applications of multivariate regression analysis, canonical correlation analysis and nonparametric statistical procedures to issues in business research involving multivariate data. Topics include building, evaluating, and validating a regression model; analyzing models using hierarchical regression, contrast coding, partial correlations and path analysis; and comparing parametric and corresponding nonparametric tests.

BUSI 6240 APPLIED MULTIVARIATE STATISTICS—Examines applications of multivariate statistical procedures involving data reduction techniques and analyzing multidimensional relationships in business research. Topics include multivariate analysis of variance, discriminant analysis, logistic regression, exploratory factor analysis, cluster analysis, multidimensional scaling and conjoint analysis.

BUSI 6280 APPLICATIONS IN CAUSAL AND COVARIANCE STRUCTURE MODELING—Focuses on specific topics including reviews of causality and path analysis, covariance algebra, creating path diagrams and structural equations, LISREL notation and syntax, considerations in model identification, estimation, evaluation and interpretation. Specific application areas include confirmatory factor analysis and its extensions, causal models with directly observed and latent variables.

3. **Research Courses (*e.g.*, individual research courses, direct studies, special topics courses, internship, and doctoral dissertation; minimum of 48 credits)**

Examples of research courses are: CSCE 5932 (INTERNSHIP), CSCE 6900 (SPECIAL PROBLEMS), SLIS 6000 (Seminar in Information Science), COMM 5185 (Quantitative Research Methods in Communication), CSCE 6940 (INDIVIDUAL RESEARCH), CSCE 5934 (DIRECTED STUDY), CSCE 6950 DOCTORAL DISSERTATION.

4. **PhD committee during the first semester:**

This committee shall consist of the student's advisor (major professor), program coordinator, and at least three additional members (*e.g.,* from CSCE, ITDS or LIS). By the end of the semester, students must submit to their committee a completed degree plan that has been approved by the Graduate School. Student shall complete all the courses, with a grade of B or higher, including theoretical courses (such as Analysis of Algorithms) recommended/approved by the student's PhD committee.

PhD Research Topics: A sample of potential research topics drawn from each department are available. Contact the program manager (Ram Dantu) for more details

Multidisciplinary Requirements: The doctoral program is intended to provide students with a variety of approaches to researching and solving information assurance problems from multiple disciplines. Therefore, the program requires students take a minimum of 12 graduate credit hours from departments other than their home department (CSCE, ITDS and LIS).

Concentration Colloquium: Upon completion of the dissertation defense, PhD candidates shall be required to present their research at a concentration colloquium. The colloquium differs from the dissertation defense as it prepares candidates to present the impacts and implications of their results to a broader audience than their committee members. Typically, this audience shall be made up of the three department's faculty and graduate students as well as other interested university members. The audience may also include appropriate experts from security industry.

Program Management

The Interdisciplinary Information Assurance PhD program will be managed by a program manager (Ram Dantu) and the faculty advisors (*e.g.,* the PhD Committee, and an advisory board from the federal agencies). Dissertation advisers (major professors) are responsible for curricular, career development and research issues for individual students. The PhD committee meets regularly to monitor students' progress, to use assessment data, and to determine needed program changes. The Admissions committee determines which students receive SFS fellowships and recommends students for other fellowships, scholarships, and awards. Program manager works with students seeking approval from the OPM and to match students with one or more advisory board members. The