Texas Higher Education Coordinating Board
Proposal for a Doctoral Program

Directions: This form requires signatures of (1) the Chief Executive Officer, certifying adequacy of funding for the new program; (2) the Chief Executive Officer, acknowledging agreement to reimburse consultants' costs; (3) a member of the Board of Regents (or designee), certifying Board of Regents approval for Coordinating Board consideration; or, if applicable, (4) a member of the Board of Regents (or designee), certifying that criteria have been met for Commissioner consideration. Additional information and instructions are available in the *Guidelines for Institutions Submitting Proposals for New Doctoral Programs* found on the Coordinating Board web site, www.thecb.state.tx.us/newprogramscertificates. Institution officials should also refer to Texas Administrative Code (TAC) 5.46, *Criteria for New Doctoral Programs.*

Note: Institutions should first notify the Coordinating Board of their intent to request the proposed doctoral program before submitting a proposal. Notification may consist of a letter sent to the Assistant Commissioner of Academic Quality and Workforce, stating the title, CIP code, and degree designation of the doctoral program, and the anticipated date of submission of the proposal.

Information: Contact the Division of Academic Quality and Workforce at (512) 427-6200.

Administrative Information

1. Institution Name and Accountability Group

Sam Houston State University

2. Program Name – *Show how the program would appear on the Coordinating Board's program inventory [e.g., Doctor of Philosophy (Ph.D.) in Electrical Engineering].*

Doctor of Philosophy (Ph.D.) in Digital and Cyber Forensic Science

3. Proposed CIP Code – *Include justification if the program title is not already included in the Texas Classification of Instructional Programs.*

11.1003 Computer and Information Security/Information Assurance

4. Program Description – *Describe the program and the educational objectives.*

The Department of Computer Science in the College of Sciences at Sam Houston State University proposes a PhD program in Digital and Cyber Forensic Science.

Sam Houston State University is a nexus of law enforcement and forensic science capability at all academic levels with existing graduate programs in Criminal Justice, Forensic Science, Digital Forensics, Information Assurance and Security, and Security Studies. The University is currently authorized to offer doctoral programs in Criminal Justice and Forensic Science. The Department of Computer Science is authorized to offer Master of Science degrees in Digital Forensics and in Information Assurance and Security. The proposed program will complement and extend these existing programs.

The number of degree programs in the United States related to digital and cyber forensics is increasing, as is the need for qualified and credentialed professionals, researchers, scientists, and academicians. To date, there are no doctoral programs in the United States targeting digital and cyber forensic science, and only two Computer Science programs at the highest level that include a component addressing forensics or cyber security. In 2011 the American Association of Forensic Sciences, Forensic Science Education Programs Accreditation Commission (AAFS/FEPAC) revised their accreditation standards for forensic science academic programs at the baccalaureate and master's level to include specific requirements or electives for digital evidence coursework including network forensics, multimedia forensics, mobile device forensics, malware analysis, and anti-forensics. [1] Meeting these standards requires terminally degreed faculty members with specialized expertise in digital and cyber forensic science.

Sam Houston State University proposes a Doctor of Philosophy (PhD) in Digital and Cyber Forensic Science as a full-time, on campus doctoral program designed to prepare individuals in the digital forensics and cyber security fields to lead the nation in the development of digital forensics and cyber security tools and techniques, in the application of novel research to address digital forensics and cyber security issues, and in post-secondary and graduate education to

prepare the next generation of educators and academicians.

The PhD program in Digital and Cyber Forensic Science at Sam Houston State University will provide students with the theoretical, conceptual, methodological, and computational skills needed to understand the role of digital and cyber forensic science in post technological societies, i.e. where technology ubiquitously and transparently underpins society. The program will allow students to explore the possibilities for forensically sound digital data capture and analysis, and to develop new tools and methods for handling digital and cyber forensic evidence. In doing so, this program has, as its primary focus, research into the computational and scientific basis for forensic and cyber technologies rather than the application of tools or protocols in a law enforcement context.

The proposed Doctor of Philosophy in Digital and Cyber Forensic Science aligns its Program Educational Objectives (PEOs) and Student Learning Outcomes: (SLOs) with accreditation standards currently in development by the Accreditation Board for Engineering Technology (ABET) and draft standard published by AAFS/FEPAC. The proposed program has three PEOs:

1. Professional Capability: Show a commitment to working on solutions to problems with global, economic, environmental, and societal impacts;
2. Leadership/Teamwork: Be successful in a range of leadership and teamwork roles; and
3. Lifelong Learning: Show a commitment to lifelong learning through the pursuit of new knowledge through a coherent and focused research agenda.

The PEOs are expected to manifest themselves in the later stages of the program and to continue to underpin the academic and professional careers of successful students as they embark on academic and research careers.

The program defines the following Student Learning Outcomes (SLOs): The successful candidate must demonstrate:

- Skills/Knowledge: The ability to apply knowledge of digital and cyber forensics techniques sufficient to provide skilled leadership in both research and academic environments;
- Problem Solving: The ability to analyze a problem, and identify and define the forensic requirements appropriate to its solution;
- Design/Implementation: The ability to design, implement, and evaluate a computer-based system, process, component, or program to meet desired Digital and Cyber Forensic Science needs;
- Leadership/Teamwork: The ability to function effectively on teams to accomplish a common goal and as a team leader;
- Law/Ethics: An understanding of professional, ethical, legal, security, and social issues and responsibilities
- Communication: The ability to communicate effectively with a range of audiences;
- Impact Analysis: The ability to analyze the local and global impact of computing on individuals, organizations, and society; and
- Professional Development: Recognition of the need for, and the ability to engage in continuing professional development.

This program will prepare 21st century forensics and cyber security leaders to guide and direct the development of more robust security systems; improve forensic analysis techniques through a research-oriented, technical, conceptual, and active learning focused program, incorporating project based learning, that addresses the security and forensic concerns at machine, network, national, and global levels; and to prepare the next generation of educators and academicians in digital and cyber forensic science.

The proposed program is designed to be a full-time, on-campus program comprising 85 credit hours consisting of 70 hours of coursework and 15 hours of dissertation.

5. Administrative Unit – *Identify where the program would fit within the organizational structure of the institution (e.g., The Department of Electrical Engineering within the College of Engineering).*

The Department of Computer Science within the College of Sciences

6. Proposed Implementation Date – *Include the first year and semester that students would enter the program.*

Spring 2018

7. Contact Person – *Provide contact information for the person who can answer specific questions about the proposed program.*

Name: Dr. Somer Franklin
Title: Assistant Vice President, Academic Affairs, Sam Houston State University
E-mail: somer@SHSU.EDU
Phone: 936.294.1009

Proposed Doctoral Program -- Required Information

I. Need

A. Job Market Need

Provide short- and long-term evidence of the need for graduates in the Texas and US job markets. Common sources for workforce need and workforce projections include the Bureau of Labor Statistics, the Texas Workforce Commission, and professional associations. If the program is designed to address particular regional or state needs in addition to workforce demands, provide a detailed description.

Lack of Digital Forensics Personnel

The lack of manpower, training, and equipment are some of the biggest concerns facing digital and cyber forensics in the United States. According to studies by The National Institute of Justice (NIJ) and the Institute for Security Technology Studies (ISTS) at Dartmouth, the law enforcement community has identified a need for more computer crime investigators, expert witnesses, digital forensic scientists, and technology/equipment to analyze digital evidence. The ISTS studies note that 41 percent of the respondents indicated that the current tools lacked essential features and 40 percent indicated that tools did not exist for functions that they needed to carry out as part of their digital investigative process. The most recent Census of Publicly Funded Crime Laboratories from the Bureau of Justice Statistics [2], noted that more than 1,200 digital evidence related forensic requests were backlogged in publicly funded forensic crime labs by year end 2008 and 2009 respectively and that backlog is only expected to increase. The examination of digital evidence was performed by the smallest percentage (19%) of publicly funded crime labs in 2009. Federal labs (44%) were more likely than state (10%), county (21%), or municipal (32%) labs to report analyzing digital evidence. This shortage in the capability to conduct digital forensic analysis on a timely basis has a profound impact on public safety. In their January 2015 newsletter, The American Society of Crime Lab Directors noted that West Virginia State Police Crime Labs are currently severely short-staffed and are now facing a 3,400-case backlog, making it difficult to support approximately 800 agencies that depend on their services. [3] Crime labs are in urgent need of digital forensic examiners, expert witnesses, digital forensic scientists, and researchers, to create tools and design investigative processes and procedures for dealing with digital evidence in an efficient manner.

Lack of Cyber Security Personnel

In February 2003, the United States Federal Government published the National Strategy to Secure Cyberspace [4], recognizing that the security and assurance of data and communications within the United States represents a critical infrastructure asset worthy of protection. The latest publication of this document [5], revised June 17, 2014, highlights the importance of securing not only physical assets, but the cyber assets of public and private institutions in a number sectors including agriculture, food, water, public health, emergency services, government, banking, finance and defense among others. Among the top five national priorities outlined in this report, is the need for increased cyber security personnel, and to create adequate training and education programs to support the nation's cyber security needs.

The Scale of the Problem

In order to address the shortfall in digital and cyber forensic science personnel, the Bureau of Justice Statistics estimated the percent increase in full-time forensic scientists needed to eliminate backlogs and prevent their recurrence. [5] In 2005 (the last full census date), the United States needs to increase the number of full-time computer crime examiners by 15 percent to achieve a 30-day turnaround.

In the 2002 and 2005 Census of Publicly Funded Laboratories, computer crime evidence requests represented the smallest itemized function. By 2009 computer crimes evidence requests exceeded those of two more traditionally itemized functions, indicating a rise in the importance of computer crime evidence processing for publicly funded laboratories. The number of request for computer crime evidence rose from 1,881 in 2005 to 31,000 in 2009. This highlights the increasing importance of the analysis of digital and cyber evidence in the investigation of crimes, and points to a future

where the shortage of credentialed and skilled examiners, expert witnesses, and the academicians needed to educate those examiners will only increase. Only 19 percent of publicly funded laboratories currently have the capacity to process computer related crime evidence.

The Bureau of Justice, Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012 [6] indicated that the total economic loss from identity theft exceeded losses from all other property crime by more than 75 percent.

TABLE 4
Mean, median, and total losses attributed to identity theft and property crime, 2012

	Mean	Median	Total (in thousands)
Identity theft[a]	$2,183	$300	$24,696,300
Property crime[b]	$915	$150	$13,991,700
Burglary	2,378	600	5,234,800
Motor vehicle theft	7,963	4,000	3,079,900
Theft	447	100	5,677,000

Note: See appendix table 6 for standard errors.

[a]Based on 11.3 million persons 16 or older who experienced one or more incidents of identity theft with known losses of $1 or more.

[b]Based on 15.3 million household property crimes, 2.2 million burglaries, 400,000 motor vehicle thefts, and 12.7 million household thefts with known losses of $1 or more. In 2012, 19% of completed burglaries had unknown loss amounts.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, 2012, and National Crime Victimization Survey, Identity Theft Supplement, 2012.

Recent years have seen significant, high profile security breaches including

2014

- P.F. Changs;
- Sally Beauty Supply (25,000 records);
- Michaels;
- Jimmy Johns;
- Neiman Marcus (1.1 million records);
- The Home Depot (56 million records);
- Target (70 million records);
- JP Morgan Chase (7 million records); and
- Sony Pictures Entertainment.

2015

- Carefirst BlueCross BlueShield (1.1 million records);
- Kaspersky Labs (Internet security company);
- Premera BlueCross BlueShield (11.2 million records);
- Multi-bank Cyberheist ($1 billion in fraudulent transfers – ongoing);
- Harvard University (18,000 records);
- Army National Guard (850,000 records);
- Anthem (80 million records); and
- Office of Personnel Management – breached twice (25.7 million records). [8]

The Ponemon Institute [8] conducts an annual Benchmark Study on Privacy and Security of Healthcare Data. The study shows a 125% increase in criminal cyberattacks on healthcare organizations since 2010. Criminal cyberattacks are the primary cause of data breaches in the healthcare industry, are experienced by healthcare organizations of all sizes, and cost the healthcare $6 billion annually.

Worldwide, Ponemon estimates that over 1 billion records were stolen in 2014. The range of attacks and data breaches encompass government, military, and commercial organizations. The average cost

of a single successful breach is $3.8 million (a 23% increase over 2013) and the average cost incurred for a single record containing sensitive information is $154.

Context and Environment

Provide short- and long-term evidence of the need for graduates in the Texas and US job markets. Common sources for workforce need and workforce projections include the Bureau of Labor Statistics, the Texas Workforce Commission, and professional associations. If the program is designed to address particular regional or state needs other than workforce demands, please identify those needs.

SHSU, uniquely within the State of Texas, has the academic expertise, organizational structures, and physical infrastructure to establish such a program. In addition to the above, SHSU has an internationally recognized graduate Criminal Justice Program, and the Department of Computer Science is the home for the only graduate Digital Forensics Program in the state of Texas. Both of these programs provide excellent training for law enforcement, for technical professionals at the state and federal level. Graduates from the Department of Computer Science's ABET/CAC accredited undergraduate Computing Science Program and Master's degree in Digital Forensics are recruited by the FBI, the Department of Homeland Security, and the Secret Service, as

In late 2004, through the foresight and support of Senator Kay Bailey Hutchison and Representative James Turner, Sam Houston State University established the SHSU Center of Excellence in Digital Forensics, a center designed to provide training to local, state, and federal law enforcement personnel and other legal professionals in the correct handling, interpretation, and presentation of digital evidence. At the national level, in December 2005, Secretary of the Air Force Michael Wynne and Chief of Staff of the Air Force General T. Michael Moseley announced an extension of the Air Force mission to include cyberspace. [10] To address increasing internet crime rates and the risk of cyber warfare and cyber terrorism, a report by the United States Joint Forces Command [11] in February 2010 stated: "Through cyberspace, enemies will target industry, academia, government, as well as the military in the air, land, maritime, and space domains. Cyberspace has fractured the physical barriers that shield a nation from attacks on its commerce and communication" (p. 36).

The growth in demand for digital forensic services in Texas has led to the establishment, as announced by FBI director Robert S. Mueller in 2003 and opened in 2005, of the Greater Houston Regional Computer Forensics Laboratory (GHRCFL). [12]

The GHRCFL is a "one-stop full-service forensics laboratory and training center devoted entirely to the examination of digital evidence in support of criminal investigations" including:

- Cyber and digital forensics;
- Terrorism;
- Child pornography;
- Violent crimes;
- Theft of and destruction of intellectual property;
- Internet crime; and
- Fraud. (www.ghrcfl.org)

According to the latest Reginal Computer Laboratory's (RCFL) Annual Report (FY 2012) [13], the GHRCFL top five computer forensic investigation requests were Exploitation/Enticement, Fraud, Homicide, Sexual Assault, and Dangerous Drugs. The center averaged a 6 percent increase in investigation requests in FY12, coupled with a 40 percent increase in the data volume processed. The demand for skilled technical personnel in law enforcement as well as in commercial service providers to business, industry, and government is increasing annually. Meeting this demand requires enhanced in-service training opportunities together with academic programs to develop the next generation of digital and cyber forensics investigators.

Recognizing that providing in-service training opportunities to the law enforcement community represented only a partial solution, the Department of Computer Science at Sam Houston State University designed, proposed, and implemented a Master of Science degree in Digital Forensics,

intended to complement and extend the undergraduate academic programs in Computing Science, Management Information Systems, and Criminal Justice. At the practical level, digital and cyber forensics concerns itself with the techniques and methodologies associated with the detection, collection, analysis, preservation, and presentation of digital evidence to support the commercial, law enforcement, and legal professions in digital fraud and criminal investigation. From an academic perspective, there is a growing demand and need for new digital tools and protocols to improve intrusion detection/recovery, network, and cyber security, and information assurance. Such needs can only be met through an advanced technical understanding of data, computer systems and communications, knowledge of the legal and justice systems, and an understanding and appreciation of the importance of the forensics process.

Digital and cyber forensics is clearly emerging as a new academic discipline [14] that combines both Computational Sciences and Criminal Justice, much in the same way that Management Information Systems emerged in the late 1970s and Geographical Information Systems in the late 1990s, first as groups of tool users and tool developers with distinct computational needs, and later as a body of theoretical knowledge, conceptual bases, and a common specialized language to analyze the threats that cybercriminals pose to our physical and cyber infrastructure.

The initial lack of training opportunities for state and local law enforcement in the fields of digital and cyber forensics has also prompted the establishment of a federally funded training facility, the National Computer Forensic Institute (NCFI). The NCFI was established in 2008, with a mandate to provide state and local law enforcement, and legal, and judicial professionals a free, comprehensive education on current cyber-crime trends, investigative methods, and prosecutorial and judicial challenges. [15]

In the National Strategy to Secure Cyberspace, the Department of Homeland Security has been charged with initiatives such as providing crisis management for response to attacks on critical information systems, providing technical assistance to private and public entities, and providing coordination with agencies concerning warning information and protective measures. Meeting this charge in the long term involves developing a state and national capacity to provide high quality training, education, and research in Digital and Cyber Forensic Science. Such a capacity requires a convergence of academic expertise in forensics systems, Emergency Management, and Computer Science at the highest levels. According to Kessler and Haggerty [16], a skilled academician and a Digital Forensics examiner, academicians play a critical role in advancing the science of digital and cyber forensics. They are in a position to help work with the practitioner community to advance standards, tools, research, legislation, and local training efforts.

The evidence of present and future vocational need for a doctoral program in digital and cyber forensics rests on three complementary arguments.

1. The first consists of an academic discussion of the needs and demands of a post technological society and the educational system that supports it;
2. The second concerns the general employment conditions for computer related professions that have a bearing on the digital and cyber forensics function; and
3. The third comprises an analysis of currently available jobs and their educational requirements.

Kessler and Haggerty stated that the development of graduate degree programs in Digital Forensics as a response to "the need for the next-generation of leaders… largely steeped in technology and computer science, preparing students for more rigorous research and development in the technical problems related to computer forensics, such as the need for more and better examination and reporting tools coping with whole disk encryption, acquiring data from cellular telephones and other mobile devices, and combating anti-forensics tools."

Yasinsac et al. [17] describe four roles within the digital forensics profession and identify the appropriate educational background:

1. Technicians, with the skills required to identify, preserve, retrieve and document digital evidence;
2. Enterprise Policy Makers, with knowledge of law, management and technical issues, and responsible for developing enterprise-level policy;
3. Forensics Professionals, responsible for implementing policy, designing protocols and communicating this to technicians; and
4. Researchers, responsible for the development of the conceptual and theoretical basis for next generation tools and protocols.

Existing undergraduate and master's level programs adequately address the technical and professional requirements of the first three roles.

A fifth role is also required. This is the role of educators, researchers, and scientists in institutions of higher education with the appropriate academic and research background necessary to provide both undergraduate and graduate education for the next generation of digital and cyber forensics examiners and practitioners. To this end, this program seeks to produce scholars who are educated in digital and cyber forensic science, who can contribute to the body of knowledge, and who can educate the next generation of digital and cyber forensics examiners.

Employment

In this section, national occupational employment and wage estimates are provided. The estimates are calculated by the Bureau of Labor Statistics using data collected from employers in all industry sectors related to Computer and Mathematical Occupations in metropolitan and nonmetropolitan areas in every State and the District of Columbia.

Because digital and cyber forensics is a relatively new area of expertise, neither the Bureau of Labor Statistics nor the Texas Workforce Commission provides statistics specifically for digital and cyber forensics employment. However, some inferences can be made to more general categories of employment such as Computer and Information Science, or Computer Security, but care must be taken in assessing these statistics in relation to a field that is still emerging.

The closest occupational categories associated with a digital and cyber forensics professional currently in use by the Bureau of Labor Statistics' Occupational Employment Training and Earnings Database (2012) were determined by using the following phrases:

- Digital Forensics;
- Digital Security;
- Computer Forensics;
- Cyber Forensics; and
- Computer Security.

The most pertinent categories derived from these keywords are:

- Computer and Information Research Scientists;
- Computer and Information Systems Managers;
- Computer Science Teachers (Post Secondary);
- Computer System Analysts;
- Information Security Analysts;
- Network and Computer Systems Administrators;
- Software Developers, Applications; and
- Software Developers, Systems.

The following data was obtained:

Title	Employment 2012	Employment 2022	2012-2022 Change (%)	Job Openings	Median Wage	Minimum Entry Education
Computer and Information Research Scientists	26,700	30,800	15.3	8,300	102,910	Bachelor's
Computer and Information Systems Managers	332,700	383,600	15.3	97,100	120,950	Bachelor's
Computer Science Teachers (Post Secondary)	41,700	47,000	12.7	11,600	72,200	Doctoral/Professional
Computer Systems Analysts	520,600	648,400	24.5	209,000	79,600	Bachelor's
Information Security Analysts	75,100	102,500	36.5	39,200	86,170	Bachelor's
Network and Computer Systems Administrators	366,400	409,400	11.7	100,500	72,560	Bachelor's
Software Developers, Application	613,000	752,900	22.8	218,500	90,060	Bachelor's
Software Developers, Systems	405,000	487,800	20.4	134,700	99,000	Bachelor's

The Texas Workforce Commission's "State of Texas Information and Computer Technology Cluster Assessment [18] (2005, citing the *AeA Cyberstates* 2005 Report) identified Texas as ranking 2nd in the nation for employment in high tech workers, 2nd also in employment in telecommunications and engineering, and 3rd in technology-oriented venture capital investments. These rankings remained the same in 2012. The report recommends (pp. 4-6) nurturing the IT cluster development and identifies eight targets of opportunity. The field of digital and cyber forensic science is directly associated with four of the eight targets (highlighted) and indirectly associated with all the others.

- Logistics/supply chain solutions;
- **Cyber security;**
- **Homeland security;**
- Digital media arts;
- **Border security;**
- **RFID/smart cards;**
- Supercomputing; and
- Wireless.

Digital forensics technicians and computer security specialists were identified as two of the targeted professions for long-term growth potential by Interlink. [19]

In a recent report, "Professionalizing the Nation's Cyber Security Workforce: Criteria for Decision-Making (2013)" by the National Academies Press [20], the committee, composed of advisors from the Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences and the National Research Council noted that while Cyber Security is, as yet, too young for the federal government to undertake its licensure "there is only one possible Cyber Security sub-field where there exists a compelling case for professionalization, that of digital and cyber forensics examiners". According to the American Academy of Forensic Sciences' Forensic Education Programs Accreditation Commission's Accreditation Standards the professionalization of digital and cyber forensic examiners would require academic credentials to the Masters' level. This, in turn, would require credentialed faculty members with terminal degrees in the field. It is exactly this area that the proposed PhD in Digital and Cyber Forensic Science is targeting.

A review of job listings on three major jobs sites was conducted in August 2015. The tables below summarize the results. The results from Dice.com are worldwide, those from Monster.com are

national with a very few international positions, and the results from Jobs.com are for the state of Texas. Monster.com and Job.com do not report listing counts above 1000.

Search Term	Dice.com (International)	Monster.com (National)	Jobs.com (Texas)
Digital Forensics	5,192	89	292
Digital Security	22,526	41	25
Computer Forensics	26,214	99	292
Cyber Security	18,526	1,000+	1,000+
Information Security	40,991	1,000+	1,000+
Cyber Forensics	1,994	141	150

Position Title	Dice.com (International)	Monster.com (National)	Jobs.com (Texas)
Computer and Information Research Scientists	2,235	5	653
Computer and Information Systems Managers	12,175	1,000+	850
Computer Systems Analysts	60,270	1,000+	1,000+
Information Security Analysts	47,475	1,000+	1,000+
Network and Computer Systems Administrators	41,805	1,000+	1,000+
Software Developers, Application	66,142	1,000+	1,000+
Software Developers, Systems	71,227	1,000+	1,000+

A review of position postings from the www.ieee.org provides the following data:

Key Phrase	Location	Position Count
Cyber Security	USA	323
Data Security	USA	1,056
Computer Forensics	USA	61
Information Assurance	USA	959

Academic and Research Positions:

A search of the jobs section of the Chronicle of Higher Education [21] revealed the following data:

Key Phrase	Faculty Positions	Administrative Positions	Executive Positions
Digital Forensics	9	1	0
Computer Forensics	4	3	0
Information Assurance	13	3	1
Cyber Security	30	5	1
Data Security	4	7	2
Total	**60**	**19**	**4**

It is clear that the digital and cyber forensics profession is emerging, the qualifications for entry into the profession are beyond the baccalaureate degree, demand for credentialed professionals is likely to rise significantly over the next ten years, and the need for both digital/cyber forensics research and education requires the development of a terminal degree in Digital and Cyber Forensics Science.

It is also clear that the State of Texas has a sufficiently advanced technology cluster that does, and will continue to rely on digital and cyber forensics services. Indications from the state reflect that the IT sector should be encouraged to develop, especially in the forensics and cyber security arenas. It is also evident that Sam Houston State University, with its existing Criminal Justice, Forensics Science, and Digital and Cyber Forensics capabilities, together with its geographical location, being

surrounded by the three largest population and employment metropolitan areas, is uniquely suited to house such a program.

B. Existing Programs

Identify the existing programs and their locations in Texas. Provide enrollments and graduates of these programs for the last five years, and explain how the proposed program would not unnecessarily duplicate existing or similar programs in Texas. Provide evidence that existing Texas programs are at or near capacity and describe how the existing programs are not meeting current workforce needs. Provide the job placement of existing Texas programs. Provide information about the number of existing programs nationally.

The Digital Forensics Association (DFA) is a non-profit organization dedicated to fostering education, providing networking opportunities and conducting research to benefit the digital forensics community. [22] They have compiled a list of ten graduate level, Masters' or equivalent, Digital Forensics (or allied area) programs in academic institutions in the United States including:

- Carnegie Mellon University;
- Champlain College;
- George Washington University;
- John Jay College of Criminal Justice;
- Marshall University;
- Purdue University (Center for Education and Research in Information Assurance and Security);
- Sam Houston State University;
- University of Central Florida;
- University of New Haven;
- University of Rhode Island; and
- Texas State University (Minor in Forensics Systems).

The following institutions offer Master's degree in fields somewhat related to Digital and Cyber Forensic Science (not listed on the Digital Forensics Association's website):

- University of Maryland University College (Cybersecurity);;
- James Madison University (Digital Forensics, Information Security);
- John Jay College of Criminal Justice (Digital Forensics and Cybersecurity);
- The University of Alabama at Birmingham (Computer Forensics and Security Management);
- American Public University (Cybersecurity studies);
- NYU-Poly (ePoly Online Graduate Program in Cybersecurity and Digital Forensics);
- University of Baltimore (MS in Forensic Science – High Technology Crime);
- University of Colorado Denver (MS in Media Forensics);
- La Salle University (MS in Economic Crime Forensics);
- Utica College (MS in Cybersecurity); and
- New Jersey Institute of Technology (MS in Cybersecurity and Privacy).

Doctoral level study that includes Digital Forensics is available at only two institutions in the United States, the University of Rhode Island, and Purdue University. Both these doctoral programs are PhD programs in Computer Science with a concentration (12 hours) that provides students the opportunity to specialize in one of several disciplines - Information Security, Cyber and Network Security, and Digital Forensics. Neither of these two programs focuses exclusively on Digital and Cyber Forensics.

There are no degree programs at the doctoral level within the United States that have a primary focus on Digital and Cyber Forensic Science. No public institutions within the state of Texas offer areas of study in Digital and Cyber Forensic Science at the doctoral level. Only Sam Houston State University (MS in Digital Forensics, MS in Information Assurance and Security) offers significant graduate level Digital and Cyber Forensics coursework.

Within the State of Texas there are a number of institutions that have the capacity to provide individual coursework in security and related areas. In particular:

- The University of Texas at San Antonio offers graduate courses in Principles of Computer and Information Security, Developing Secure Systems and UNIX and Network Security. However, it does not offer any courses related to Digital Forensic Science nor does it offer an area of emphasis in Digital and Cyber Forensic Science;
- Texas A&M University offers one graduate course in Advanced Networking and Security and two courses in Information, Secrecy and Authentication. However, it does not offer any courses related to Digital and Cyber Forensic Science;
- The University of Texas at Dallas hosts the Digital Forensics and Emergency Preparedness Institute but does not offer academic coursework at the undergraduate or graduate level in Digital Forensics;
- The University of North Texas offers two graduate courses; an Introduction to Computer Security, and Secure Electronic Commerce, but no specific Digital Forensics coursework and no areas of study in Digital Forensics;
- The University of Texas at El Paso offers one graduate course in Computer Security at the graduate level; and
- The University of Houston offers one graduate course in Data Security at the graduate level.

C. Student Demand

Provide short- and long-term evidence of student demand for the program. Types of data commonly used to demonstrate this include increased enrollment in related and feeder programs at the institution, high enrollment in similar programs at other institutions, qualified applicants rejected at similar programs in the state, and student surveys. Provide documentation that qualified applicants are leaving Texas for similar programs in other states.

Enrollment in Computer Science, Digital Forensics, and Information Assurance and Security

The Department of Computer Science has pursued a program of quality enhancement over the past five years, with comprehensive reviews of both undergraduate and graduate curricula and the development of a more research oriented faculty leading to the ABET/CAC accreditation [23] of our undergraduate Computing Science degree program.

The undergraduate degree program in Computing Science consists of a 26 credit hour core containing essential theoretical and practical skills that are recognized as vital to the computer science profession. In addition, the degree program requires 18 hours of specialized computer science coursework, 15-17 hours of Mathematics and 16 hours of Science. The curriculum meets or exceeds guidelines established by the two significant curriculum bodies in Computing Science, ABET/CAC and the Association for Computer Machinery (ACM). [24]

Although undergraduate Computer Science programs have risen steadily since a 20-year low in 2007, current enrollment and degree production at the national level is 25% below 2001 levels. [25] In contrast, the Baccalaureate degree in Computing Science at Sam Houston State University has shown an average year-on-year growth of 6 percent since 2002. This can be attributed to two primary causes, first the accreditation status of the degree program and the quality this implies, and second, the existence of the graduate degree programs in Digital Forensics and Information Assurance and Security, which acts as a draw to potential students.

The Department of Computer Science offers graduate degree programs in three areas: Computer Information Systems (CIS), Digital Forensics (DF) and Information Assurance and Security (IAS), the last of which is a new program that began in Fall 2009. The department has been successful in maintaining its traditional CIS program as well as developing and growing new programs to meet demand.

The areas of specialty most directly related to doctoral study in Digital and Cyber Forensic Science are the current MS in Digital Forensics and MS in Information Assurance and Security. The enrollment in the MS in Digital Forensics was 10 in Fall 2012 but has increased to 21 in Fall 2014. The MS in Information Assurance and Security attracts approximately 35 percent of all current graduate enrollment within the Department of Computer Science. The MS in Information Assurance and Security commenced in fall 2009 with 2 students and Fall 2014 active enrollment was 34.

Over the most recent 5-year period, the Digital Forensics and Information Assurance and Security programs have shown a total growth of 139 percent, equivalent to an annualized growth rate of 14.7 percent.

Sam Houston State University has seen significant growth in demand for computer science and for programs related to the proposed program, namely forensic science and criminal justice. Since 2003 the number of declared majors in the baccalaureate computing science program has more than doubled. THECB statistics indicate that more than 80 percent of all students graduating from the program are employed, and/or enrolled in a graduate or professional program (latest figures 2009-2011).

Student enrollment in the Forensic Science MS program at SHSU increased more than 100 percent between 2006 and 2012. In 2012, fifteen students graduated from the MS program, compared with 7 in 2006. The graduate student enrollment for the last nine years is detailed in Table below.

Graduate Student Enrollment by Program 2005-2014	CIS	DF	IAS	Total
2005	23	0	0	23
2006	28	17	0	45
2007	21	22	0	43
2008	32	18	0	50
2009	35	16	2	53
2010	37	17	13	67
2011	39	12	13	64
2012	24	12	24	60
2013	26	26	36	88
2014	35	21	34	90

The Computer Science Department Graduate Curriculum Committee conducted a survey during Summer 2015. A total of 250 undergraduate and graduate students in Computer Science and Digital Forensics were contacted and asked to complete the survey. A total of 57 students were responded (22.8%).

Of those respondents, 44.6 percent indicated that they were Very or Extremely Interested in the proposed program. 86 percent of respondents indicated that financial support was either "Important" or "Vital" to them pursuing a PhD in Digital and Cyber Forensics Science. Thirty-one percent indicated that a PhD in Digital and Cyber Forensic Science was Very Important to their personal goals. 30 percent indicated that a PhD in Digital and Cyber Forensic Science was Vital to their Professional Goals. The tables below provide more detailed responses to the five specific questions. Note that the question numbers are the actual ones used in the survey.

Q1: How interested are you in pursuing a doctoral program in Digital and Cyber Forensic Science?

Answer Choices	Respondents	Percentage
Not Interested	3	5.36%
Somewhat Interested	28	50.00%
Very Interested	20	35.71%
I've been looking for someone to start this program.	5	8.93%
Total	**56**	**100%**

Q2: How important is financial support in deciding to pursue a PhD in Digital and Cyber Forensic Science?

Answer Choices	Respondents	Percentage
Not Important at all	1	1.75%
Not Important, but it would be nice to have	7	12.28%
Important but not vital	14	24.56%
Essential	35	61.40%
Total	**57**	**100%**

Q3: How important is it for courses within the program to be online?

Answer Choices	Respondents	Percentage
Not Important	9	15.79%
Useful but not Necessary	22	38.60%
Important	16	28.07%
Vital	10	17.54%
Total	**57**	**100%**

Q6: How important would a PhD in Digital and Cyber Forensic Science be to your personal goals?

Answer Choices	Respondents	Percentage
Not Important	13	22.81%
Somewhat Important	26	45.61%
Very Important	18	31.58%
Total	**57**	**100%**

Q7: How important would a PhD in Digital and Cyber Forensic Science be to your professional goals?

Answer Choices	Respondents	Percentage
Not Important	13	22.81%
Somewhat Important	26	45.61%
Very Important	18	31.58%
Total	**57**	**100%**

D. Student Recruitment

Describe recruitment efforts specific to the proposed program, including plans to recruit and retain students from underrepresented groups.

The Department of Computer Science has a well-developed recruitment strategy at all levels that leverages:

- Institutional support from the University's marketing department, enrollment management and graduate admissions;
- Recruitment by faculty and graduate students through presentations at professional meetings;

- Institutional and Departmental funding of marketing materials;
- Promotion of newsworthy events through the University, College, and department websites together with local and State newspapers; and
- Promotion of the programs through federal and state law enforcement agencies and business and industry through the SHSU Center of Excellence in Digital Forensics.

The master's level programs in Digital Forensics and Information Assurance and Security have already achieved national recognition. The Information Assurance and Security program has ranked in the top ten in the nation for online technology graduate programs annually since 2012. The effects of this recognition can be seen in the increase in enrollment since 2012. The Digital Forensics program has produced competitive teams for the Department of Defense Cybercrime challenge. Students in the Digital Forensics and Information Assurance and Security programs are actively engaged in research and publication and provide service to local and state law enforcement. The Digital Forensics program has been successful in placing students in internships with the FBI and commercial organizations. Graduates from the programs are employed in federal law enforcement, business and industry, and local and state government.

The Department of Computer Science maintains a database of Computing Science, Digital Forensics, and Information Assurance and Security students and alumni tracking internship and employment data. The following tables provide recent internship and employment data for students and alumni of the Digital Forensics and Information Assurance and Security programs.

Internships since 2011

First Name	Last Name	Internship	Employment Status	Program Status
Todd	Redacted	FBI Honors Internship	DF analyst, FBI	Continuing
Eric	Redacted	Huntsville Police Dept.	Sys Admin. SHSU	Continuing
Kevin	Redacted	FBI Honors Internship	Graduate Assistant, SHSU	Continuing
Johnny	Redacted	Hewlett-Packard		Continuing
Subash	Redacted	Computerized Assessment/Learning		Completed
Sundar	Redacted	Indusoft	No	Continuing
Ugo	Redacted	Univ. Alabama CRIME Lab	Alert Logic	Continuing
Ugo	Redacted	Univ. Alabama CRIME Lab	Alert Logic	Completed
Raviteja	Redacted	Crowdsoft	Unknown	Completed
Anna	Redacted	Texas DPS Cybersecurity	None	Continuing
Drew	Redacted	Texas DPS Cybersecurity	None	Continuing
Andrew	Redacted	Texas DPS Cybersecurity	None	Continuing
Kimberley	Redacted	Alliance Data	None	Continuing
Samantha	Redacted	Intuit	None	Continuing
Michaila	Redacted	Huntsville Police Department	None	Continuing

Partial Employment Data Since 2011

First Name	Last Name	Organization	Job Title	Sector
Pat	Redacted	T-Systems	IT risk Analyst	
Hugh	Redacted	Gardenier & Associates	Partner, CPA, CFE, CFF	Accounting
Martha	Redacted	Gardenier & Associates	Partner, CFA, CPA, CFF	Accounting
Faraz	Redacted	CitiGroup	Assistant VP, Global Data Center Automation	Banking
James	Redacted	Udacity	Course Manager	Education
Julie	Redacted	Baker College	Adjunct Faculty	Education
Tracie	Redacted	Huntsville ISD	Director of Technology	Education
Steven	Redacted	SHSU	Director of Technology	Education
Tim	Redacted	SHSU	Information Security Officer	Education
Marilyn	Redacted	SHSU	Information Security Analyst	Education
Kirk	Redacted	SHSU	Instructor	Education
Eric	Redacted	SHSU	Systems Admin. I	Education
Andrew	Redacted	SHSU	Director, CEDF	Education
Avinash	Redacted	Shelby County	Web Developer	Government
David	Redacted	N.O.A.A.	IT Specialist	Government
Todd	Redacted	FBI	Redacted	Government
Cynthia	Redacted	New York Life Ins.	Agent	Insurance
Steve	Redacted	Occidental Petroleum	IT Security Engineer	Oil & Gas
Matt	Redacted	National Oilwell Varco	Director of Automation and Control Engineering	Oil & Gas
Kevin	Redacted	CyberPoint International	Incident Response Lead	Security
David	Redacted	Deloitte	Senior Associate	Security
Mary	Redacted	Gumshoe Investigative	Owner	Security
David	Redacted	Engagency	Developer	Technology
Matthew	Redacted	Schlumberger- SIS	Systems Engineer – PTCi	Technology
Ugo	Redacted	Alert Logic	System Security Analyst	Technology
Noe	Redacted	Hewlett Packard	OPS/Engineer	Technology
Johnny	Redacted	Hewlett Packard	Programmer	Technology
Alex	Redacted	CISCO	Systems Engineering Manager	Technology
Stephen	Redacted	Bazaarvoice	Front End Software Engineer	Technology
Alex	Redacted	Microsoft Dynamics CRM	Security, Privacy & Compliance	Technology
Brittany	Redacted	Alert Logic	Security Engineer	Technology
Dathan	Redacted	Palantir Technologies	Forward Deployed Software Engineer	Technology
Christopher	Redacted	MediaFire.com	Software Developer	Technology
Michael	Redacted	Dell	Engineer-Virtualization	Technology
D.J.	Redacted	Verizon	Cyber Security Engineer	Telecomm.

E. Enrollment Projections

Use Table 1 to show the estimated cumulative headcount and full-time student equivalent (FTSE) enrollment for the first five years of the program, including the ethnic breakdown of the projected enrollment (White, African American, Hispanic, International, Other). Include summer enrollments, if relevant, in the same year as fall enrollments. Subtract students as necessary for projected graduations or attrition. Provide explanations of how headcounts, FTSE numbers, projections for underrepresented students, and attrition were determined. Define full-time and part-time status.

Table 1. Enrollment Projections**

	Year 1	Year 2	Year 3	Year 4	Year 5
New Students	7	8	8	9	10
White	5	5	5	5	6
African-American	1	1	1	2	2
Hispanic	1	2	2	2	2
International	0	0	0	0	0
Other	0	0	0	0	0
Cumulative Headcount	7	15	23	31	40
FTSE*	10.5	19.4	26.3	30.9	33.8
Attrition	0	0	1	1	1
Graduates	0	0	0	0	6

*Per the THECB University Accountability Measures and Definitions, the FTSE's for the doctoral level are based on 9 semester credit hours (SCH) per each fall/spring semester or 18 semester credit hours (SCH) per academic year. That definition assumes that students will take classes only in the fall and spring semesters, so there are no SCH expectations for summer sessions. The proposed program requires 6 credit hours of internship in the first year of the program. As a result, FTSE count is greater than the cumulative headcount. FTSE counts are derived from the THECB's Program Funding Estimation Tool.

Each year in the chart above represents cohorts of 7-10 candidates (multiple cohorts after Year 1), with each candidate enrolled in nine SCH in the fall semester, nine SCH in the spring semester, and six SCH in the summer.

**Based on an analysis of current ethnic and gender representation in the Digital Forensics and Information Assurance and Security programs.

Explanation of How Headcount and FTSE Numbers Are Determined

The projected estimates will likely ensure program success. The projection of 5-7 new doctoral candidates beginning each calendar year is based on historical evidence of other doctoral programs at Sam Houston State University. The projected numbers of doctoral candidates in the table reflect a growth curve, which builds enrollment gradually so at the end of 5 years, the program should be well publicized and self-sustaining.

The estimated attrition rates are likely appropriate. The attrition of one student per year, beginning in year 2 is consistent with existing doctoral programs at SHSU. The University has excellent support services for existing doctoral students and a successful history of retention and completion. Utilizing the experiences of two colleges housing existing doctoral programs (the College of Education and the College of Criminal Justice), the Office of Graduate Studies, the College of Sciences, and the Department of Computer Science will work to develop and maintain an aggressive marketing effort, while keeping the student population at a level that stresses individual

attention and high quality instruction. In particular, once students in the program attain candidacy, support for candidates' successful completion of the program will include:

- Advisement by program faculty;
- Supervision and consultation by the candidate's dissertation chair; and
- Collaboration among program faculty in support of candidates.

II. Academics

Opportunities for Research

The research philosophy of the doctoral program in digital and cyber forensics is two-fold: First to promote the interdisciplinary scientific research and development and second, to promote industry and government collaborations.

Digital forensics research at SHSU is already interdisciplinary in nature with collaborations between the department of computer science and the college of criminal justice, in particular law enforcement training in digital evidence protocols, development of the CRIMES communication system, and the establishment of the Center of Excellence in Digital Forensics. Since 2005 the department of computer science has attracted more than $3 million in federal and local funding through National Science foundation (NSF), Department of Justice (DOJ), and National Institute of Justice (NIJ) programs. The proposed PhD program would make SHSU more competitive in terms of federal awards and assistance. In addition to state, local, and federal funds in support of forensic science and related research, students at SHSU would be eligible for the PhD Graduate Research Fellowship (GRF) program of the (NIJ). These competitive awards support research on crime, violence, and other criminal justice-related topics within accredited academic universities that offer research-based doctoral degrees in disciplines relevant to NIJ's mission.

The Department of Computer Science has established industry research collaborations including Sierra Nevada Corporation, Indusoft, Ricoh Forensics, Palo Alto Laboratories, NFS Laboratories and AccessData. Government collaborations include the greater Houston Regional Computer Forensics Laboratory, Huntsville Police Department, Trinity, Walker, and Harris County sheriff's offices, and the Texas Rangers division of the Texas Department of Public Safety.

Access to the necessary resources for rigorous scientific research is a major advantage of these partnerships. Linking operational laboratories and productive research programs provides a basis for a proactive and forward-looking profession. The academic-industrial partnerships that already exist at SHSU will ensure that research in the PhD program will have a direct benefit to the field of Digital and Cyber Forensic Science

A. Accreditation

If the discipline has a national accrediting body, describe plans and timeline to obtain accreditation. For disciplines where licensure of graduates is necessary for employment, such as nursing, plans for accreditation are required. If the program will not seek accreditation, provide a detailed rationale explaining why.

At this time there are no national or regional accreditation organizations that would accredit a digital and cyber forensic science program at the doctoral level. AAFS/FEPAC has developed accreditation standards for undergraduate and masters level digital evidence programs. Those standards require that at least 50 percent of the full-time faculty teaching in such programs must have an appropriate terminal degree, preferably in Digital and Cyber Forensic Science. Therefore, at the national level, in order to develop, implement, and maintain accreditation-worthy undergraduate and graduate programs in Forensic Science, Digital Forensics, and Cyber Forensics, a cadre of terminally degreed faculty members with Digital and Cyber Forensic Science credentials must be developed.

The National Security Agency (NSA), in partnership with the Department of Homeland Security, designates centers for Academic Excellence in Information Assurance, Cyber Defense, and Cyber Operations. While this does not rise to the level of accreditation, it will be an important step for the Master's degree programs in Digital Forensics and Information Assurance and Security, and the

proposed doctoral degree program in Digital and Cyber Forensic Science to achieve as a measure of program quality.

B. Admissions Standards

Describe the institution's general graduate admissions standards and the program-specific admissions standards for applicants of the program. The description addresses how the proposed program will seek to become nationally competitive. Explain how students will be assessed for readiness to enroll in program coursework. Include any policies for accepting students transferring from other graduate programs. Explain whether the program will accept full-time and part-time students.

Applicants for admission into the Doctoral Program in Digital and Cyber Forensic Science must have an earned Baccalaureate or Master's degree in Digital Forensics, Information Assurance, Computer Science, Computer Engineering or similar field that includes the foundational knowledge required for the proposed program. Documentation of the applicant's graduation from an accredited institution at the Baccalaureate or Masters level will be required.

Applicants must submit one of the following:

- An acceptable combined score on the verbal and quantitative sections of the Graduate Record Examinations. The test must be taken within 5 years the program application. Acceptable scores are determined by the following formula: V x 0.5 + Q x 1.5 >300; and
- An official transcript indicating successful completion of a Baccalaureate or Master's degree in Digital Forensics, Information Assurance, Computer Science, Computer Engineering, or a similar field.

Additional requirements are as follows:

- A current resume or curriculum vita;
- An official transcript of all undergraduate and graduate coursework;
- Three letters of recommendation from either an accredited institution of higher education or from a related professional setting; and
- An interview conducted by the graduate faculty of the Computer Science Department, in which the candidate demonstrates the technical foundations required for the program and a commitment to applied research.

Students who previously graduated from the Master of Science programs in either Digital Forensics or Information Assurance and Security may incorporate up to 30 semester credit hours towards the doctoral degree with approval from the Graduate Advisor in the Department of Computer Science following recommendations from the Digital and Cyber Forensic Science Advisory Committee. A maximum of 12 semester credit hours may be transferred from graduate programs from universities other than SHSU with approval from the Graduate Advisor in the Department of Computer Science following recommendations from the Digital and Cyber Forensic Science Advisory Committee in accordance with university policies.

C. Program Degree Requirements

Describe the similarities and differences between the proposed program and peer programs in Texas and nationally. Indicate the different credit hour and curricular requirements, if any, for students entering with a bachelor's degree and students entering with a master's degree. Use Table 2 to show the degree requirements of the program. If requirements vary for students entering with a master's degree or comparable qualifications, provide an explanation. Modify the table as needed. If necessary, replicate the table to show more than one option.

There are no peer programs across the country. As described earlier, only two doctoral programs in computer science exist that address significant digital and cyber forensics course content, and that is

limited to a 12-hour concentration. The proposed program includes the content offered in those programs but significantly extends that content in both breadth and depth. The proposed program does address the academic content identified in the AAFS/ FEPAC Accreditation standards, and addresses the academic and research focus identified by the National Security Agency's Center of Academic Excellence program in Cyber Operations.

Table 2: Program Degree Requirements

Category	Semester Credit Hours, Entering with Bachelor's	Semester Credit Hours, Entering with Master's
Required Courses	49	28
Prescribed Electives	15	6
Electives		
Dissertation	15	15
Other (Specify, e.g., internships, clinical work, residencies)	6	6
TOTAL	85	55

Note: The semester credit hours identified for applicants entering with a Master's degree are calculated on the assumption that the graduate degree is either in Digital Forensics or Information Assurance and Security, and that the coursework associated with the Master's degree addresses appropriate content, in particular:

- Digital Forensic Tools;
- File System Forensics;
- Network Forensics;
- Law;
- Criminalistics;
- Operating System Forensics and Security;
- Cryptography and Steganography;
- Malware Analysis; and
- Cyber Warfare.

Complete Table 3 to provide a comparison of the proposed program to existing and/or similar programs in Texas in terms of total required semester credit hours. Modify the table as needed.

Table 3. Semester Credit Hour Requirements of Similar Programs in Texas

Institution	Program CIP Code	Degree Program	Semester Credit Hours, Entering with Bachelor's	Semester Credit Hours, Entering with Master's
Texas A&M University	11.0701	Computer Science	94	64
Texas State University*	11.0701	Computer Science	72	42
University of Texas at San Antonio	11.0701	Computer Science	90	60
University of Texas at Dallas**	11.0701	Computer Science	73	43
University of North Texas***	11.0701	Computer Science	72	42

University of Texas at El Paso	11.0701	Computer Science	72	33

* The credit hours specified by Texas State University do not include dissertation hours.
** The University of Texas at Dallas specifies 3 hours of dissertation as a minimum requirement.
*** The credit hours specified by the University of North Texas do not include dissertation hours.

D. Curriculum

Describe the educational objectives of the proposed program. If the program has a unique focus or niche, describe it in relationship to peer programs. Describe how the program would achieve national prominence. Provide an explanation of required, prescribed, and elective courses and how they fulfill program requirements.

Describe policies for transfer of credit, course credit by examination, credit for professional experience, placing out of courses, and any accelerated advancement to candidacy. Identify any alternative learning strategies, such as competency-based education, that may increase efficiency in student progress in the curriculum. If no such policies are in place to improve student progression through a program, provide an explanation.

Complete Tables 4, 5, and 6 to list the required/core courses, prescribed elective courses, and elective courses of the program and semester credit hours (SCH). Note with an asterisk (*) courses that would be added if the program is approved. Modify the tables as needed. If applicable, replicate the tables for different tracks/options.

The proposed Doctor of Philosophy in Digital and Cyber Forensic Science has three Program Educational Objectives (PEO's) identified on page 2 of this proposal:

The PEO's are expected to manifest themselves in the later stages of the program and to continue to underpin the academic and professional careers of successful students as they embark on academic and research careers.

The curriculum for the proposed program is based on the philosophy that a comprehensive and rigorous curriculum at the highest level should balance five essential components:

- Theory
- Systems
- Application
- Professional Environment
- Research

To make such a balance both explicit and understandable the Digital and Cyber Forensic Science Doctoral Development Committee (consisting of the Computer Science Department Chair and two member of the Graduate (full Doctoral) faculty) has designated the course coding in the following way:

- Digit 1 indicates the level of the course (university-wide).
- Digit 2 indicates the number of credit hours (university-wide).
- Digit 3 indicates the nature of the course based on the above philosophy (program-specific).
- Digit 4 indicates preferred sequence. Within each of the five components identified above the fourth digit identifies the order in which the courses should be taken. Higher numbers indicate courses that are taken later in the program.

The first two digits are compliant with course coding across the university. The third digit characterizes the primary focus of each course as follows:

- 0 – courses that may address any of the philosophical components
- 1 – Breadth-first courses
- 2 - Professional Environment
- 3 /4 - Application
- 5 – Theory/Systems
- 6/7 – Research

Table 4. Required/Core Courses

Prefix and Number	Required/Core Course Title	SCH
DFSC 6410	Cyber Forensics Principles*	4
DFSC 7300	E-Discovery*	3
DFSC 7340	DF Tools & Techniques*	3
DFSC 5316	File System Forensic Analysis	3
DFSC 7352	Network Forensic Analysis*	3
DFSC 7106	Seminar in Digital Forensics * (x4)	4
DFSC 7600	Internship*	6
FORS 5226	Law and Forensic Science	2
FORS 6094	Criminalistics for Digital Forensics	3
DFSC 7350	Operating System Forensics*	3
DFSC 7320	Ethics for Digital Forensics*	3
DFSC 7362	Computational Forensics*	3
DFSC 7358	Live System & Memory Forensics*	3
DFSC 7356	Mobile Device Forensics*	3
DFSC 7360	DF Research Methods*	3
DFSC 7364	Scientific Communications*	3
DFSC 7330	DF Laboratory Management*	3
DFSC 8370	Dissertation* (continuous enrollment)	15

Table 5. Prescribed Elective Courses		
Prefix and Number	**Prescribed Elective Course Title**	**SCH**
DFSC 7359	Social Network Forensics*	3
COSC 5310	Cryptography and Steganography	3
DFSC 7357	Malware Forensic Analysis*	3
DFSC 7341	DF Infrastructure*	3
DFSC 6310	Cyber Warfare and Terrorism	3
DFSC 7351	Cloud Computing Forensics*	3
DFSC 7353	RAID & Remote System Forensics*	3
DFSC 7355	Intrusion Forensic Analysis*	3
DFSC 7365	Commercial Tool Verification*	3

Table 6. Elective Courses		
Prefix and Number	**Elective Course Title**	**SCH**
Not Applicable. The program does contain elective courses.		

The following matrix identifies the expected percentage of time allocated within each course in the core and elective courses to each of the philosophical components (aggregate numbers are rounded and may not sum to exactly 100%).

Prefix and Number	Theory	Systems	Application	Environment	Research
DFSC 6410	34%	33%	33%		
DFSC 7300		34%	66%		
DFSC 7340			67%	33%	
DFSC 5316	33%	34%	33%		
DFSC 7352	34%	66%			
DFSC 7106	20%	20%	20%	20%	20%
DFSC 7600		33%	33%	34%	
FORS 5226			50%	50%	
FORS 6094			50%	50%	
DFSC 7350	50%	50%			
DFSC 7320				100%	
DFSC 7362	66%				34%
DFSC 7358	50%	50%			
DFSC 7356		50%	50%		
DFSC 7360			50%	50%	

DFSC 7364			34%		66%
DFSC 7330			50%	50%	
DFSC 8370					100%
Core balance	**16%**	**21%**	**32%**	**23%**	**12%**
DFSC 7359	34%	33%			34%
COSC 5310	33%	34%			33%
DFSC 7357	33%		34%		33%
DFSC 7341			50%	50%	
DFSC 6310		50%	50%		
DFSC 7351	34%	33%			33%
DFSC 7353	34%	33%			33%
DFSC 7355	33%	34%	33%		
DFSC 7365	25%	25%			50%
Elective balance*	**28%**	**27%**	**19%**	**6%**	**21%**
Total balance*	**16%**	**20%**	**23%**	**15%**	**26%**

* Students will take 15 hours of electives. The balance across philosophical components within the electives and overall will vary depending on the specific elective selected.

The Curriculum Schematic below provides additional detail.

Semester	Curriculum Schematic		Cumulative
Semester 1 (Spring 20xx) Core Coursework (**11** credit hours)	FORS 6094 Criminalistics for Digital Forensics DFSC 6410 Cyber Forensics Principles DFSC 7300 E-Discovery DFSC 7106 Seminar in Digital Forensics	[3] [4] [3] [1]	**11** credits
Semester 2 (Summer 20xx) Core Coursework (**6** credit hours)	DFSC 7600 Internship	[6]	**17** credits
Semester 3 (Fall 20xx) Core Coursework (**10** credit hours)	DFSC 5316 File System Forensic Analysis DFSC 7352 Network Forensic Analysis DFSC 7340 DF Tools & Techniques DFSC 7106 Seminar in Digital Forensics	[3] [3] [3] [1]	**27** credits
Semester 4 (Spring 20xx) Core Coursework (**9** credit hours)	FORS 5226 Law and Forensic Science DFSC 7350 Operating System Forensics DFSC 7320 Ethics for Digital Forensics DFSC 7106 Seminar in Digital Forensics	[2] [3] [3] [1]	**36** credits
Semester 5 (Fall 20xx) Core Coursework (**10** credit hours)	DFSC 7362 Computational Forensics DFSC 7358 Live System & Memory Forensics DFSC 7356 Mobile Device Forensics DFSC 7106 Seminar in Digital Forensics	[3] [3] [3] [1]	**46** credits
Advancement to Candidacy	**Portfolio Review Comprehensive Examination**		**Unsuccessful candidates may be allowed to complete the requirements for the MS Degree.**
Semester 6 (Spring 20xx) Core Coursework (**9** credit hours)	DFSC 7360 DF Research Methods DFSC ------ Electives DFSC 8370 Dissertation	[3] [3] [3]	**55** credits
Semester 7 (Fall 20xx) Core Coursework (**9** credit hours)	DFSC 7364 Scientific Communications. DFSC ------ Electives DFSC 8370 Dissertation	[3] [3] [3]	**64** credits
	Dissertation Proposal Defense		
Semester 8 (Spring 20xx) Core Coursework (**9** credit hours)	DFSC 7330 DF Laboratory Management DFSC ------ Electives DFSC 8370 Dissertation	[3] [3] [3]	**73** credits
Semester 9 (Fall 20xx) Core Coursework (**6** credit hours)	DFSC ------ Electives DFSC 8370 Dissertation	[3] [3]	**79** credits
Semester 10 (Spring 20xx) Core Coursework (**6** credit hours)	DFSC ------ Electives DFSC 8370 Dissertation	[3] [3]	**85** credits
	Formal Public Seminar **Dissertation Defense**		

Accelerated Advancement towards Candidacy

The proposed program allows for the transfer of credit from other institutions.

- Up to 12 hours of relevant graduate coursework may be transferred from an accredited institution of higher education.
- Up to 30 hours of relevant coursework may be applied from a completed Master's degree in Digital Forensics or Information Assurance and Security awarded by Sam Houston State University.

Alternative Learning Strategies

The proposed program requires students to engage in the following as a means of providing competency-based experiences to enhance and complement course-based learning:

- At least one year of research development as a member of the university's Center of Excellence in Digital Forensics; and
- One full-time summer internship.

E. Candidacy/Dissertation

If the proposed program requires a dissertation, describe the process leading to candidacy and completion of the dissertation. Describe policies related to dissertation hours, such as a requirement to enroll in a certain number of dissertation hours each semester. Indicate if a master's degree or other certification is awarded to students who leave the program after completing the coursework, but before the dissertation defense.

A dissertation is required in the proposed PhD in Digital and Cyber Forensic Science.

In consultation with faculty and student, each candidate in the proposed program will be assigned to a doctoral faculty advisor who is a member of the doctoral faculty in the program area. The candidate will work closely with the doctoral faculty member to acquire and develop experience in the development of grounded research projects. Decisions about advisement will rest with the doctoral faculty member and the program administrator. An online documentation process will be utilized to maintain a continuous record of advisement conferences and specific actions. Candidates will be assigned to doctoral faculty advisors who can provide guidance about topical content for dissertation research projects, perhaps leading to the faculty advisor becoming either a member or chair of the candidate's dissertation committee.

Advisors will present options in course offerings and specify a course of study for doctoral candidates. It will be the responsibility of the advisor to communicate the candidate's course of study to the graduate school and the principal administrator.

Students will be reviewed for candidacy at the end of their second year in the program after completing a total of 46 credit hours of course work including all but six hours of the core courses identified in the program together with a six-hour (full-time summer) internship. The review process involves:

- Comprehensive examination
- A Portfolio Review

Comprehensive Examinations

Comprehensive examinations are conducted for students completing their second year of the program. The comprehensive examinations combine, written, oral, and laboratory testing, and address all five essential program components: theory, systems, applications, professional environment, and research.

- **Theory** – This component tests student familiarity and understanding of fundamental concepts, principles, classifications, and methodologies in digital and cyber forensic science. This component is evaluated through written and oral exams.
- **Systems** – This component tests student understanding of the interconnections and interactions among the various elements in the body of knowledge and practices and are addressed in written, laboratory, and oral examinations.
- **Application** – This component examines the students' skills and capabilities in applying theory, systems, and methods to the solution of real problems. This area is primarily addressed in the laboratory examination.
- **Professional environment** – This component examines the students' familiarity with the professional environment including processes, procedures, professional communication, and ethics. This area is primarily addressed in laboratory and oral examinations.
- **Research** – This component examines the student's knowledge and understanding of the research process including scientific literacy, research methodology, and trends in digital and cyber forensic science. It is mostly covered in the oral examination.

A student must obtain a passing grade in all five components to receive an overall pass in the comprehensive examination. A retest is given by the end of the following semester on any previously failing components. If a student fails a second time on the same component, termination of the program is warranted.

Portfolio Review

In order to monitor the quality of the proposed doctoral program and evaluate student performance, the doctoral faculty committee will conduct a mandatory formal portfolio review at the end of the second year. Each student is required to document coursework, research, and skills acquisition. Where appropriate, teaching experience will be documented. In order to progress towards candidacy, the student's portfolio must meet minimum requirements in each of the areas:

- **Coursework** – Each student will provide a summary report of all courses taken and their performance, together with research papers developed as part of their coursework and any resulting published materials. Students are also expected to reflect on their performance and identify strengths and weaknesses, and develop a plan of action to address any areas of concern through the judicious selection of elective courses during their third and fourth years. Students are expected to meet a minimum GPA of 3.33 during their first two years and to be able to demonstrate a growing capability for scientific writing.
- **Research** – Each student will document their primary research activities, findings, and outcomes in the first two years. These should include, but not be limited to, research foci, research projects and roles, presentations, publications of article or journal submissions, and possibly citations. While a doctoral student at this stage may not necessarily have published scholarly works, there should be sufficient evidence to indicate that the student has been actively involved in serious research and making progress towards dissertation. Minimum requirements are clearly identified research interests and foci, records of scholarly paper reading and summaries, and at least two submissions to regional or international conferences or journals. A strong portfolio may also include published, peer-reviewed scholarly work(s) and presentations to international conferences and venues.
- **Skills Acquisition** – Each student will self-evaluate the development of professional skills including programming, tool use, systems, written and oral communications, and teamwork and collaboration. Students should demonstrate continuous skills acquisition together with increasing sophistication in the application of those skills.
- **Teaching** – Where relevant, student teaching experience, as a teaching assistant or instructor, should also be included in the portfolio submission. Student will document any courses taught, class sizes, primary teaching methods, tools, and skills used, and teaching evaluation where applicable.

Candidacy

Following successful completion of the portfolio review and comprehensive examinations students will continue to year three of the program including 6 hours of dissertation preparation. Students will, through discussion with doctoral faculty, identify an appropriate dissertation chairperson, and dissertation committee. At a point determined by the dissertation chairperson, the student will be directed to defend the dissertation proposal to the dissertation committee.

The student must prepare a formal written proposal describing the research. The research proposal must be an outline of the dissertation project. It must include a summary of the project, the hypotheses to be investigated, significance, research design and methodology, limitations, and a review of relevant literature.

A committee comprised of at least four faculty members will perform the review. At least two members of the committee shall be graduate faculty in Computer Science with responsibilities within the doctoral program. One member of the committee may be from the College of Criminal Justice. One committee member must be external to the Department of Computer Science and must be a member of the graduate faculty in the College of Sciences.

If the proposal defense is satisfactory, the student may advance to doctoral candidacy. Doctoral students who are not successful may be dismissed or allowed to complete the requirements for a Master of Science degree.

At this time, a doctoral student who does not wish to advance to candidacy may petition the Digital and Cyber Forensic Science Advisory Committee to complete the requirements for a Master of Science in Digital Forensic degree

During year four, doctoral candidates must maintain continuous enrollment until the dissertation has been completed and submitted for review in accordance with institutional policy. The defense of the completed dissertation requires approval from the candidate's dissertation committee, a formal public presentation, and an oral defense of the dissertation, together with meeting the university requirements for review and finalization by the Office of Graduate studies and the University Library.

F. Use of Distance Technologies

If applicable, describe the use of any distance technologies in the program, including a description of interactions between students and faculty, opportunities for students to access educational resources related to the program, exchanges with the academic community, and in-depth mentoring and evaluation of students. If more than 50 percent of the program content will be delivered off-campus, the institution must also submit a completed "Distance Education Doctoral Degree Proposal" form: Distance Education Degree Doctoral Form.

This program is intended to be full-time face-to-face. However, all courses will make use of Distance Learning technologies to enhance, rather than replace in class instruction. The University's Learning Management System provides a number of key tools that can, in conjunction with the classroom, provide state of the art instruction including; recording of class sessions for later review, discussion boards to extend material presented in class, and community and small group facilities for team-based projects.

G. Program Evaluation

Describe how the program will be evaluated. Describe any reviews that would be required by an accreditor, and show how the program would be evaluated under Board Rule 5.52.

Where applicable, the program will be evaluated in accordance with the Graduate Program Standards of the AAFS/FEPAC and the NSA's Requirements for Designation as a Center of Academic Excellence in Cyber Operations. In accordance with those standards, a graduate Digital and Cyber Forensics Science program shall provide advanced education in the scientific and laboratory problem

solving skills necessary for success in a modern DF laboratory. The program must combine rigorous scientific and laboratory training with exposure to the breadth of digital and cyber forensic science disciplines, including digital and cyber forensic science practice, law enforcement, and ethics. Additionally, the doctoral program will quantitatively evaluate its performance using institutional measures of effectiveness in terms of publication rate, postgraduate employment success and employer satisfaction.

The program will be reviewed as part of the ongoing SHSU periodic academic program review process. This process involves intensive self-study complemented by an external assessment conducted by disciplinary experts. The doctoral program will be subjected to this review every five years.

In section D.1 the Program Education Objectives and Student Learning Outcomes were identified. The Department of Computer Science has developed assessment tools both to measure the effectiveness of the curriculum and departmental advisement systems to achieve the PEO's and SLO's over the long-term, and to feedback assessment results into the curriculum for continuous improvement.

The following table describes how Student Learning Outcomes map to the Program Educational Objectives.

	Professional Capability	**Leadership/Teamwork**	**Lifelong Learning**
Skills/Knowledge	✓	✓	
Problem Solving	✓	✓	✓
Design/Implementation	✓		
Leadership/Teamwork		✓	✓
Law/Ethics	✓	✓	✓
Communication	✓	✓	
Impact Analysis		✓	✓
Professional Dev.	✓	✓	✓

A Doctoral Advisory Committee will be formed comprising:

- The Principle Program Administrator;
- A member of the Forensic Science doctoral faculty;
- A member of the Digital and Cyber Forensic Science core faculty;
- A member from the commercial/professional realm; and
- A member from a national government agency concerned with digital and cyber forensic science.

The Doctoral Advisory Committee will conduct an annual interview with each doctoral candidate to obtain information that will result in specific program improvement recommendations.

Program Formative Measures

The program will examine multiple measures to assess program quality including:

- Admission and retention rates (each semester);
- Access to historically underrepresented groups;
- Annual review by the Doctoral Advisory Committee ;
- The generation of published research involving doctoral faculty and program students and candidates;
- Portfolio review with respect to research, leadership and evidence of academic development; and

- Student and candidate satisfaction surveys, particularly with respect to progress on the SLOs.

Program Summative Measures

The Computer Science office will maintain the files of successful graduates and maintain contact with those graduates to develop records on placement and advancement over time. Annual follow-up questionnaires, e-communication, and phone conversations will provide information and data on the success of graduates. The department will use data from graduates on the types of professional positions, job satisfaction, and impact of the doctoral credential to structure curricular and mentoring decisions for program improvement. Evaluation will be directed toward ascertaining how doctoral graduates of the program are influencing and directly contributing to the profession, to furthering research, and to preparing the next generation of digital and cyber forensics professionals.

Program Review

In accordance with Board Rule 5.52, the proposed program will be subject to external review on a 7-year cycle. Sam Houston State University has developed policies and guidelines for the review process including:

- The construction of a self-study report evaluating Program Profile, Administration, Curriculum, Faculty Resources and Credentials, Student Success, Resources, Assessment, and Marketing;
- A timeline for the program review process;
- The identification and recruitment of external reviewers; and
- The development of an action plan for improvement.

Student Learning Objective Measurement

Student Learning Objective measurement will be implemented through the following performance indicators:

- Progress in IDEA Objectives;
  - 21 – 24 (Skills and Knowledge);
  - 25 (Leadership/Teamwork);
  - 29 and 31 (Problem Solving/Design/Implementation);
  - 30 (Law/Ethics);
- Comprehensive Examinations;
- Portfolio Review; and
- Dissertation Proposal and Final Defense.

H. Strategic Plan

Describe how the proposed doctoral program fits into the institution's overall strategic plan, and provide the web link to the institution's strategic plan. Explain how the proposed program builds on and expands the institution's existing recognized strengths.

The goals identified in the SHSU 2014 Strategic Plan are:

1. Foster a lifelong learning environment in support of a diverse faculty and staff who are excellent scholars, educators, and professionals;
2. Promote a stimulating learning environment through the integration of academic settings, campus culture and service;
3. Increase and develop university resources and infrastructures that support the intellectual transformation of students;
4. Enhance marketing outreach and visibility to include academic and scholarly activities through consistent and integrated messaging while optimizing communication channels;
5. Promote efficient data driven decision-making through the integration of centralized data analysis, review and dissemination; and
6. Cultivate a continually sensitive and proactive response to the ever-changing needs of our constituents.

The proposed doctoral program would address goals 1, 2, and 3 of the 2014 Institutional Strategic plan.

Through the development of the proposed program would provide an opportunity for further study at the highest level in digital and cyber forensics together with the development of a targeted and sustained research capability that would encourage lifelong study, research, and development.

The proposed program would provide a stimulating learning environment through enhanced instructional techniques involving face-to-face instruction from the highest quality faculty, continuous communication through the University's learning management system and a focus on research both in the classroom and in the laboratory.

The proposed program would enhance the intellectual and academic resources in digital and cyber forensics providing a significantly greater concentration of expertise in the field than in any other institution in the State, in the Nation, and possibly worldwide. Students entering the program would be transformed from entering professionals to high quality researchers, innovators, and academic and potentially policy leaders.

Web site: http://www.shsu.edu/dotAsset/53bef4a9-b816-4a56-afe2-86c9f6e3863c.pdf

I. Related and Supporting Programs

Complete Table 7 with a list of all existing programs that would support the proposed program. This includes all programs in the same two-digit CIP code, and any other programs (graduate and undergraduate) that may be relevant. Include data for the applications, admissions, enrollments, and number of graduates for each of the last five years. Modify the table as needed. The example provided in Table 7 shows degree programs that would relate to or support an additional Ph.D. in another area of chemistry, for example a proposal for a PhD in Forensic Chemistry (40.0510).

Table 7. Related and Supporting Programs

	2010-11	2011-12	2012-13	2013-14	2014-15
BS in Computing Science					
Applications	115	300	294	344	342
Admissions	103	242	231	267	257
Enrollment	228	272	291	316	320
Graduates	29	30	37	26	45
MS in Computing and Information Science					
Applications	63	36	43	73	78
Admissions	48	30	32	42	23
Enrollment	55	39	28	31	39
Graduation Rate	**Entering Cohort F09 Graduated until Sum11**	**Entering Cohort F10 Graduated until Sum12**	**Entering Cohort F11 Graduated until Sum13**	**Entering Cohort F12 Graduated until Sum14**	**Entering Cohort F13 Graduated until Sum15**
2 Year Graduation Rate	**40.0%**	**50.0%**	**50.0%**	**0.0%**	**60.0%**
	Entering Cohort F06 Graduated until Sum11	**Entering Cohort F07 Graduated until Sum12**	**Entering Cohort F08 Graduated until Sum13**	**Entering Cohort F09 Graduated until Sum14**	**Entering Cohort F10 Graduated until Sum15**
5 Year Graduation Rate	**50.0%**	**100.0%**	**71.4%**	**100.0%**	**66.7%**
MS in Digital Forensics					

Applications	15	11	19	12	21
Admissions	13	9	14	9	11
Enrollment	21	16	17	20	26
Graduation Rate	**Entering Cohort F09 Graduated until Sum11**	**Entering Cohort F10 Graduated until Sum12**	**Entering Cohort F11 Graduated until Sum13**	**Entering Cohort F12 Graduated until Sum14**	**Entering Cohort F13 Graduated until Sum15**
2 Year Graduation Rate	**33.3%**	**50.0%**	**40.0%**	**0.0%**	**62.0%**
	Entering Cohort F06 Graduated until Sum11	**Entering Cohort F07 Graduated until Sum12**	**Entering Cohort F08 Graduated until Sum13**	**Entering Cohort F09 Graduated until Sum14**	**Entering Cohort F10 Graduated until Sum15**
5 Year Graduation Rate	**66.7%**	**25.0%**	**66.0%**	**100.0%**	**100.0%**

MS in Information Assurance and Security					
Applications	12	25	26	33	15
Admissions	11	24	23	29	8
Enrollment	1	25	35	45	32
Graduation Rate	**Entering Cohort F09 Graduated until Sum11**	**Entering Cohort F10 Graduated until Sum12**	**Entering Cohort F11 Graduated until Sum13**	**Entering Cohort F12 Graduated until Sum14**	**Entering Cohort F13 Graduated until Sum15**
2 Year Graduation Rate	**0.0%**	**100.0%**	**19.0%**	**0.0%**	**29.0%**
	Entering Cohort F06 Graduated until Sum11	**Entering Cohort F07 Graduated until Sum12**	**Entering Cohort F08 Graduated until Sum13**	**Entering Cohort F09 Graduated until Sum14**	**Entering Cohort F10 Graduated until Sum15**
5 Year Graduation Rate	**NA**	**NA**	**NA**	**100.0%**	**100.0%**

J. Existing Doctoral Programs

Provide the web link(s) for the *18 Characteristics of Doctoral Programs* for each of the institution's existing doctoral programs. Describe how existing closely related doctoral programs would enhance and complement the proposed program.

(a) The web link for the 18 Characteristics of Doctoral Programs for each of Sam Houston State University's existing doctoral programs can be found at: http://www.shsu.edu/~grs_www/18Characteristics.html

(b) The University currently has seven doctoral programs in operation:

- PhD in Criminal Justice;
- PhD in Clinical Psychology;
- EdD in Educational Leadership;
- PhD in Counselor Education;
- EdD in Literacy;
- EdD in Instructional Technology; and
- PhD in Forensic Science.

The data available on the 18 Characteristics demonstrate that each program supports rigorous and high quality doctoral education. Each program is represented with strong numbers of

graduates, graduation rates, student and faculty publications, and other quality indicators. Although the programs differ in scope, size, purpose, and age, each existing doctoral program demonstrates a commitment to programmatic rigor while also demonstrating commitment to the success of students enrolled in the program.

(c) Two of the existing doctoral programs reside in the College of Criminal Justice, the PhD in Criminal Justice and the PhD in Forensic Science. The doctoral program in digital and cyber forensic science will complement the PhD programs in forensic science and criminal justice and afford additional opportunities for intellectual collaboration, external funding, and interdisciplinary research. There is a growing national interest in the social science-forensic science interface and existing collaborations between the departments of computer science, forensic science, and criminal justice will benefit directly from the proposed doctoral program.

K. Recent Graduates Employment

For existing graduate programs (master's and doctoral) within the same two-digit CIP code in the most recent year, show the number and percentage of graduates employed within one year of graduation, and list graduates' field of employment, location, and the employer.

The Department of Computer Science offers three graduate programs within the same two-digit CIP code as the proposed program: Computer and Information Science, Digital Forensics, and Information Assurance and Security.

For the most recent 12-month period (January 1st – December 31st 2015) the department graduated 42 Master's degree students, of which information is available for 31graduates. Of those, 28 are currently employed (90.3%) in field. For specific individuals the following organization, position, and location information is available:

Redacted, Shaun:	Employer Confidential by Request – CA
Redacted, Patrick:	DPIS Engineering LLC – Chief Technical Officer - TX
Redacted, Brittany:	Ernst & Young – Senior Consultant - TX
Redacted, Nathaniel:	U.S. Army – Captain - CA
Redacted, Alexander:	Hewlett Packard – Systems Software Engineer - TX
Redacted, Michael:	Atlmerich & Payne – Infrastructure Manager -OK
Redacted, Rakesh:	SHSU – Datacenter Operations Specialist - TX
Redacted, Ferdiansyah:	Petrolink – Real-Time Dept. Manager - TX
Redacted, Ugochukwa:	FBI – Analyst - AL
Redacted, Luke:	Anadarko – ITS Security Admin - TX
Redacted, Guo:	Deloitte – E-Discovery Consultant - TX
Redacted, J.:	CircSoft – Chief software Architect
Redacted, Joshua:	Methodist Health System – Lead Network Engineer - TX
Redacted, Marissa:	Hewlett Packard – Incident Responder - TX
Redacted, Kevin:	FBI – Digital Forensics Analyst - TX
Redacted, Leighton:	Raytheon – Senior InfoSys Technician - FL
Redacted, Michael:	Microsoft – Security Analyst - WA
Redacted, Victor:	SHSU – Cyber Security - TX
Redacted, Sundar:	WiPro – Senior Consultant - TX
Redacted, Sravan:	Saleforce – Developer - VA
Redacted, Venkata:	Apttus – Professional Services Associate - CA
Redacted, Subash:	Computerized Assessment & Learning LLC – Developer - KA
Redacted, Eloho:	SHSU – Web and Media Developer - TX
Redacted, Bupendar:	PF Chang's China Bistro – Senior Oracle DBA - AZ
Redacted, Avinash:	Selby County Government – Senior Programmer – TN
Redacted, Shannon:	Groves Industrial Supply – Software Developer - TX
Redacted, Troy:	Hewlett Packard – Software Engineer - TX
Redacted, Melvin:	Employer Confidential by Request - Germany

III. Faculty

A. Faculty Availability

Complete Tables 8 and 9 to provide information about core and support faculty. There should be at least four FTE faculty for a new doctoral program. Add an asterisk (*) before the names of the individuals who will have direct administrative responsibilities for the program. Add a pound symbol (#) before the name of any individuals who have directed doctoral dissertations or master's theses. Modify table as needed.

Table 8. Core Faculty

Name and Rank of Core Faculty	Highest Degree and Awarding Institution	Courses Assigned in Program	% Time Assigned to Program
# Shashidhar, Narasimha Assistant Professor Computer Science	PhD in Computer Science, University of Connecticut	DFSC 6410, DFSC 7300, DFSC 7350, DFSC 7353, DFSC 7355, DFSC 7356, DFSC 7358, DFSC 7364, DFSC 7365	62%
# Liu, Qingzhong Assistant Professor Computer Science	PhD in Computer Science, New Mexico Institute of Mining and Technology	DFSC 7106, DFSC 7340, DFSC 7341, DFSC 7350, DFSC 7351, DFSC 7352, DFSC 7353, DFSC 7355, DFSC 7356	87%
*# Cooper, Peter (Administration) Professor and Department Chair of Computer Science	PhD in Higher and Adult Education, University of Missouri-Columbia	DFSC 7106, DFSC 7320, DFSC 7330, DFSC 7355, DFSC 7357, DFSC 7358, DFSC 7360, DFSC 7364, DFSC 8370	52%
Karabiyik, Umit Assistant Professor Computer Science	PhD in Computer Science, Florida State University	DFSC 6410, DFSC 7106, DFSC 7300, DFSC 7340, DFSC 7341, DFSC 7350, DFSC 7352, DFSC 7358, DFSC 7359, DFSC 7362, DFSC 7330, DFSC 7351, DFSC 7355, DFSC 7364	58%
Projected new Core Faculty in Year 2016/7	PhD in Computer Science	DFSC 6410, DFSC 7300, DFSC 7350, DFSC 7353, DFSC 7355	50%

Table 9. Support Faculty

Name and Rank of Support Faculty	Highest Degree and Awarding Institution	Courses Assigned in Program or Other Support Activity	% Time Assigned to Program
# Varol, Cihan Associate Professor Computer Science	PhD in Computer Science, University of Arkansas, Little Rock	DFSC 6410, DFSC 7330, DFSC 7350, DFSC 7351, DFSC 7353, DFSC 7355, DFSC 7365	27%
# Zhou, Bing Assistant Professor Computer Science	PhD in Computer Science, University of Regina, Canada	DFSC 7320, DFSC 7330, DFSC 7362	24%
# An, Min Kyung Assistant Professor Computer Science	PhD in Computer Science, University of Texas at Dallas	DFSC 7340	20%
# Cho, Hyuk Associate Professor Computer Science	PhD in Computer Science, University of Texas at Austin	DFSC 7106, DFSC 7362, DFSC 7360, DFSC 8370	27%
Projected New Support Faculty in Year 2017/18	PhD in Computer Science	DFSC 7164, DFSC 7362, DFSC 7364, DFSC 7220	20%

B. Teaching Load

Indicate the targeted teaching load for core faculty supporting the proposed program. Teaching load is the total number of semester credit hours in organized teaching courses taught per academic year by core faculty, divided by the number of core faculty at the institution the previous year. Provide an assessment of the impact the proposed program will have, if approved, on faculty workload for existing related programs at the institution.

The teaching load calculations are based on a model 5-year scheduling plan based on a cohort of students entering in the spring of each year. It is assumed that all core courses will be taught on an annual basis, and, beginning the third year, all elective courses (highlighted in the left-hand column) will be taught on a two-year rotation.

Five-year Model Schedule

Total FTE costs for the proposed program are identified in program in the following tables. Note that the following calculations have been made:

	2018			2019			2020			2021			2022		
	Spring	Summer	Fall	Spring	Summer	Fall	Spring	Summer	Fall	Spring	Summer	Fall	Spring	Summer	Fall
FORS 6094	21			24			24			27			30		
DFSC 6410	28			32			32			36			40		
DFSC 7300	21			24			24			27			30		
DFSC 7106	7		7	15		15	15		16	17		17	19		18
DFSC 7600		42			48			48			54			60	
DFSC 5316			21			24			24			27			30
DFSC 7352			21			24			24			27			30
DFSC 7340			21			24			24			27			30
FORS 5226				14			16			24					
DFSC 7350				21			24			24					
DFSC 7320				21			24			24					
DFSC 7362						21			24			24			27
DFSC 7358						21			24			24			27
DFSC 7356						21			24			24			27
DFSC 7360							21			24			24		
DFSC 7359							21						24		
DFSC 7351							21						24		
COSC 5310									21						24
DFSC 7357									21						24
DFSC 7353										42					
DFSC 7355										42					
DFSC 7341												28			
DFSC 6310												28			
DFSC 7365												28			
DFSC 7364									18			28			24
DFSC 7330										21					
DFSC 8370							18	18	18	42	42	27	51	51	57

- An open position exists within the department. This position will be filled by fall 2016.
- An additional FTE is requested for fall 2018.
- Over the first five years of the proposed program six students from the program will be allocated teaching responsibilities in service courses and undergraduate programs within the department. This deducts 3.00 FTE from the load cost of the proposed program.
- Four courses within the program are currently part of the Masters programs in Information Assurance and Security and Forensic Science. This deducts 0.67 FTE from the load cost of the proposed program

The faculty schedule and workload for the first five years are detailed below:

	Faculty Workload					
Hours	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year5**	**Average**
Cooper	11%	44%	44%	44%	67%	42%
Karabiyik	44%	67%	67%	67%	67%	62%
Liu	0%	67%	67%	67%	67%	53%
Shashidhar	67%	78%	44%	67%	67%	64%
Open CS 1	0%	44%	44%	67%	67%	44%
An	0%	0%	0%	11%	56%	13%
Cho	0%	0%	33%	33%	33%	20%
Varol	0%	0%	0%	44%	67%	22%
Zhou	0%	0%	0%	33%	33%	13%
New CS 1	0%	0%	33%	33%	67%	27%
New CS 2	0%	0%	0%	33%	33%	13%
FORS	33%	56%	56%	56%	56%	51%
Total FTE	**1.56**	**3.56**	**3.89**	**5.56**	**6.78**	
Final FTE Requirement:						**6.8**

In the fifth and subsequent years of operation the teaching load cost of the program is 6.8 FTE per academic year. Offsetting those costs are the following:

- The Department of Forensic Science has agreed to offer FORS 6094 and FORS 5226 utilizing existing faculty resources within that department. This reduces the annual load cost by .56 FTE.
- The Department of Computer Science offers four courses as part of its current Digital Forensics and Information Assurance and Security programs. These courses should not be counted as increased workload. This reduces the annual load cost by .67 FTE.
- The Department of Computer Science anticipates the allocation of two new FTE's as part of the resourcing of the proposed program. This offsets the annual load cost by 2.00 FTE.
- The Department of Computer Science has hired Dr. Umit Karabiyik to support both the proposed program and the graduate programs in Digital Forensics and Information Assurance and Security. The offsets the annual load cost by 1.00 FTE.
- Graduate Assistantships generated by the proposed program will provide 3.00 FTE of additional teaching capacity. This allows for a reallocation of faculty to the PhD in Digital and Cyber forensics. This offsets the load cost by 3.00 FTE.

As a result, the proposed program has a net gain of 0.43 FTE for the department load, which will allow for growth in other programs without additional costs.

	Spring/Summer 2018	2018/19	2019/20	2020/21	2021/22
Administration	0.13	0.25	0.25	0.25	0.25
Core Faculty	1.23	3.00	3.44	3.22	3.22
Support Faculty			0.33	1.54	2.16
FORS	(0.33)	(0.56)	(0.56)	(0.56)	(0.56)
Graduate Assistants	0.00	(1.00)	(2.00)	(3.00)	(3.00)
Clerical/Support Staff	0.67	1.00	1.00	1.00	1.00
Total FTE	**3.36**	**5.81**	**7.58**	**9.57**	**10.19**
Net Dept. FTE	**2.36**	**3.61**	**2.54**	**3.57**	**3.07**

Supervision for the program and the Center of Excellence in Digital Forensics will be the responsibility of the program administrator. The program administrator will perform the following roles: leadership and oversight for curricular content; establishing program rigor; achievement of desired outcomes; serve on SHSU Doctoral Advisory Council; liaison between graduate faculty, the Department Chair, and the Dean of the College; and continuous communication with Coordinating Board members about programmatic fidelity, program accountability, continuous improvement, and curricular issues. In order to oversee administrative and educational function the new program will incur a load cost of .25 FTE.

Supervision for the program and the Center of Excellence in Digital Forensics will be the responsibility of the program administrator. The program administrator will perform the following roles: leadership and oversight for curricular content; establishing program rigor; achievement of desired outcomes; serve on SHSU Doctoral Advisory Council; liaison between graduate faculty, the Department Chair, and the Dean of the College; and continuous communication with Coordinating Board members about programmatic fidelity, program accountability, continuous improvement, and curricular issues. In order to oversee administrative and educational function the new program will require the re-allocation of .25 FTE.

C. Core Faculty Productivity

Complete Tables 10 and 11 to provide information about faculty productivity, including the number of publications and scholarly activities and grant awards. Table 10 shows the most recent five years of data by core faculty, including the number of discipline-related refereed papers/publications, books/book chapters, juried creative/performance accomplishments, and notices of discoveries filed/patents issued. Table 11 shows the number and amount of external grants by core faculty.

Where relevant to performing arts degrees, major performances or creative endeavors by core faculty should be included. Examples are provided below. Do not include conference papers, reviews, posters, and similar scholarship. The format of the tables and information may vary, as long as the information is conveyed clearly. Include a list of the key journals in the field.

Table 10: Total Faculty Publications and Other Scholarly/Creative Accomplishments for the Past Five Years

Faculty Name	Refereed Papers	Book Chapters	Books	Juried Creative/ Performance	Patents
Shashidhar, Narashima	11	3	0	0	0
Liu, Qingzhong	20	4	0	0	3
Cooper Peter	4	1	0	0	0
Karabiyik, Umit	2	0	0	0	0
Cho, Hyuk	8	0	0	0	2
An, Min Kyung	10	0	0	0	0
Varol Cihan	14	2	0	0	0
Zhou, Bing	8	3	0	0	0

Table 11. External Grant Awards for the Past Five Years

Faculty Name	Grant Source	Grant Subject	Dates	Total Grant Amount	Institutional Amount
Liu, Qingzhong, Cooper, Peter	National Institute of Justice	Development and Quantitative Evaluation of Steganalysis and Digital Forgery Detection Systems	2010-2013	$331,056	$331,056
Liu, Qingzhong,	National Science Foundation	Novel Detection Approaches with Comprehensive Hybrid Intelligent Systems for Multimedia Forensics	2014-2016	$249,997	$249,997

IV. Resources

A. Student Financial Assistance

Complete Table 12 to provide the number of full- and part-time students who would be funded and the anticipated amounts for each of the first five years. Modify the table as needed to distinguish between Teaching Assistantships, Research Assistantships, and Scholarships/Grants. If student financial assistance is reliant upon grant funding, explain how funding will be consistently sustained if grant income falls short of projections.

Additionally, show how the level of student support compares to the anticipated overall student cost of tuition and fees.

Table 12. Student Financial Assistance

		Year 1	Year 2	Year 3	Year 4	Year 5
Teaching Assistantships	# of Full-time students	0	2	4	6	6
	Amount per student	$20,000	$20,000	$20,000	$20,000	$20,000
	# of Part-time students	0	0	0	0	0
	Amount per student	$0	$0	$0	$0	$0
Research Assistantships	# of Full-time students	5	9	14	20	26
	Amount per student	$20,000	$20,000	$20,000	$20,000	$20,000
	# of Part-time students	0	0	0	0	0
	Amount per student	$0	$0	$0	$0	$0
Scholarships	# of Full-time students	7	15	23	31	40
	Amount per student	$1000	$1000	$1000	$1000	$1000
	# of Part-time students	0	0	0	0	0
	Amount per student	$0	$0	$0	$0	$0

Student financial support is projected at $103,500 in year 1 rising to $621,000 in Year 5.

Projected costs are based on the following assumptions:

- Teaching and Research assistantships will be used to encourage the most highly qualified doctoral students. The Research Assistants will be assigned to core faculty under the aegis of the Center of Excellence in Digital Forensics.
- Scholarships will be awarded to students who exceed the entrance requirements in a competitive manner based on GRE scores, undergraduate and graduate scholarly records, and interviews by core faculty members.

Based on the 2015-2016 catalog, tuition and fees for the 2016- 2017 academic year (the latest figures available are:

- Fall (9 hours): $3606.50
- Spring (9 hours): $3606.50
- Summer (6 hours): $2426.00

Tuition and fees represents approximately 53% of financial assistance awarded to students admitted into the program.

B. Library Resources

Provide the library director's assessment of both paper and electronic library resources for the proposed program. Describe plans to build the library holdings to support the program. Include the amount allocated to the proposed program.

The Newton Gresham Library provides access to a collection of over 1.2 million books and journals. The library also offers access to a variety of electronic resources including licensed books, journals, and bibliographic/full text databases. Specifically, the Library subscribes to 202 electronic databases, most of which include access to full text articles and chapters. In addition, the library has access to more than 45,000 full text articles and almost 50,000 electronic books. A fully operational interlibrary loan system allows students access to library resources from across the country. The Virtual Reference Desk provides students with a real-time access librarian who can demonstrate how to successfully search a database, help develop a research strategy, or suggest appropriate resources on a given topic. Current holdings in the library are fully adequate for this program, although additional holdings, particularly electronic versions, will be added if deemed necessary.

C. Facilities and Equipment

Describe the availability and adequacy of facilities and equipment to support the proposed program. Describe plans for new facilities, improvements, additions, and renovations.

The Center of Excellence in Digital Forensics

The Center of Excellence in Digital Forensics (CEDF) is the primary delivery mechanism for computing resources required by the proposed program. SHSU's Center of Excellence in Digital Forensics is dedicated to preparing digital forensics professionals through teaching, training, and research to developing cutting edge new approaches in the detection, preservation, and analysis of digital evidence. The Center also provides databases to facilitate digital forensic profiling and digital fraud investigation and maintains a wide array of industry standard software and hardware tools to improve data detection/recovery and network security. In all, the Center maintains approximately 3500 square feet of flexible lab space designed to support graduate, doctoral and faculty research. Founded in 2004, the CEDF is actively involved with local-, state-, and national- level organizations including the Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), High Tech Crime Investigators Association [26], Infragard, and the National White Collar Crime Center (NW3C) [27], among others. The CEDF has been involved in setting the agenda for Digital and Cyber Forensics Education and training for NW3C and their curriculum formed the basis for this nationally prominent training program.

Since 2011 the CEDF has established a host of new industry and public partnerships that have been pivotal in expanding CEDF's sphere of influence and access to information, resources, and research opportunities. The Center has already established local, state and national prominence that is continually expanding. The proposed doctoral program would work with the CEDF to further research into the computational and scientific basis for forensic technology by engaging the doctoral research faculty and students in projects and partner initiatives that would have a direct impact on digital and cyber forensics as whole.

Current CEDF relationships include:

- FBI: in particular, the Greater Houston Regional Computer Forensics Laboratory;
- Texas Rangers;
- Walker County Law Enforcement;
- Sierra Nevada Corporation;
- Access Data;
- Ricoh Forensics;
- Palo alto Laboratories;
- NFS Laboratories; and
- Texas DPS Cybersecurity.

The CEDF currently operates a variety of systems that would be leveraged and developed in order to meet the needs of the program including:

- 2 Data Centers
  - White Hall Data Center with a 10-core server rack, 8TB storage, a firewalled Gigabit connection and a separate DSL line
  - AB1 Data Center with a 36-core, server, 25 TB Storage Area Network, 256 GB internal main memory, and a high speed (Gigabit), protected network connection
- 3 fixed laboratories including an offline malware laboratory (120+ nodes); and
- 2 mobile laboratories (40 nodes)

The AB1 Data Center delivers a VMWare Virtual farm with resources accessible to both on- and off-campus faculty and students.

The CEDF will provide approximately 3500 sq. ft. of research and office space to students in the proposed program. Existing office space in Academic Building I and the CEDF facility in White Hall can accommodate approximately 18 doctoral students. Doctoral students have access to research facilities in Academic Building I including a functional network laboratory, a virtualization facility, and forensics workstations equipped with industry standard forensics and security tools.

D. Support Staff

Describe plans, if any, to increase or reallocate support staff in order to provide sufficient services for the projected increases in students and faculty.

It is anticipated that one permanent full-time staff member will be required in order to handle the clerical and support duties required by this program. Given the complexity of the position this will require an Administrative Assistant II position.

E. External Learning

If applicable, describe the plans for providing Internships, Clerkships, Clinical Experiences, or other required external learning opportunities. Explain the impact this new program would have, if approved, on the available number of external learning opportunities in Texas for this type of program.

The proposed program includes 6 hours of Internship taken during the summer of year 1 of the program. The Department of Computer Science has established internship relationships with:

- Austin Department of Public Safety, Cybersecurity Division
- Huntsville Police Department
- Alert Logic Inc.
- CGI

In addition, both undergraduate and graduate students have been consistently successful in obtaining summer internships with the FBI, including six internship positions in the last three years.

F. List of Potential Consultants

Provide the names and contact information for six potential consultants to review the proposed program. Consultants must come from top-ranked programs in the nation, hold the rank of full professor or senior administrator, and have no conflicts of interest relating to the proposed program. Describe concisely the qualifications of each consultant.

Institution's Proposed Consultants:

1. **Name:** Dr. Hany Farid **Title and Rank:** Professor and Department Chair
   Institution: Dartmouth College
   Phone #: 603.646.2761 **Email:** farid@cs.dartmouth.edu
   Qualifications/Expertise:
   Digital Forensics, Image Analysis, Human Perception

2. **Name:** Dr. Kenji Yoshigoe **Title and Rank:** Professor and Department Chair
   Institution: University of Arkansas at Little Rock
   Phone #: 501.569.8138 **Email:** kxyoshigoe@ualr.edu
   Qualifications/Expertise:
   Privacy and Security in Big Data

3. **Name:** Dr. Ravi Sandu **Title and Rank:** Executive Director and Chief Scientist
   Institution: Institute for Cyber Security, University of Texas at San Antonio
   Phone #: 210.458.6081 **Email:** Ravi.sandhu@utsa.edu
   Qualifications/Expertise:
   Cyber Security Models and Systems, Security Architectures, Secure E-Commerce

4. **Name:** Dr. Sujeet Shenoi **Title and Rank:** F.P. Walter Professor of Computer Science
   Institution: University of Tulsa
   Phone #: 918.631.3269 **Email:** sujeet@utulsa.edu
   Qualifications/Expertise:
   Critical Infrastructure Protection, Cyber Operations, Cyber Security, Digital Forensics

5. **Name:** Dr. Sudhir Aggarwal **Title and Rank:** Professor of Computer Science
   Institution: Florida State University
   Phone #: 850.644.0164 **Email:** sudhir@cs.fsu.edu
   Qualifications/Expertise:
   Digital and Network Security, Cybersecurity, Cybercrime

6. **Name:** Dr. Vassil Roussev **Title and Rank:** Professor of Computer Science

Institution: University of New Orleans

Phone #: 508.280.2405 **Email:** vassil@roussev.net

Qualifications/Expertise:

Cybersecurity, Privacy, Digital Forensics

G. Five-Year Costs and Funding Sources Summary

On the attached forms, provide estimates of new costs to the institution related to the proposed program and provide information regarding sources of the funding that would defray those costs. Use the Program Funding Estimation Tool found on the Coordinating Board web site (www.thecb.state.tx.us/newprogramscertificates) and attach a saved copy of the completed Excel spreadsheet to your application.

H. Signature Page

Select and obtain required signatures for either the signature page entitled, "Institutional and Board of Regents Consideration by the Board" or the signature page "Board of Regents Consideration by the Commissioner."

V. Required Appendices

A. Course Descriptions and Prescribed Sequence of Courses
B. Five-Year Faculty Recruitment Plan/Hiring Schedule
C. Institution's Policy on Faculty Teaching Load
D. Itemized List of Capital Equipment Purchases During the Past Five Years
E. Librarian's Statement of Adequate Resources
F. Articulation Agreements with Partner Institutions
G. Curricula Vitae for Core Faculty
H. Curricula Vitae for Support Faculty
I. Letters of Support from Peer Institutions and/or Area Employers

References

[1] American Association of Forensic Science/ Forensic Science Educations Programs Accreditation Commission. "FEPAC Accreditation Standards". (2014). Retrieved from http://www.fepac-edu.org/sites/default/files/FEPAC%20Standards%2002192015.pdf

[2] Bureau of Justice Statistics. Census of Publicly Funded Forensics Crime Laboratories, 2009. Retrieved from http://www.bjs.gov/content/pub/pdf/cpffcl09.pdf.

[3] Society of Crime Lab Directors "The Crime Lab Minute" Newsletter. 2015. Retrieved from http://www.ascld.org/wp-content/uploads/2015/01/CLM-January-19-2015.pdfAmerican

[4] US-CERT. The National Strategy to Secure Cyberspace. (2003). Retrieved from http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf

[5] US-CERT. The National Strategy to Secure Cyberspace. (2014). Retrieved from https://www.us-cert.gov/security-publications/national-strategy-secure-cyberspace

[6] Bureau of Justice Statistics. Census of Publicly Funded Forensic Laboratories. (2008). Retrieved from http://www.bjs.gov/content/pub/pdf/cpffcl05.pdf

[7] Bureau of Justice Statistics. Victims of Identify Theft. (2013). Retrieved from http://www.bjs.gov/index.cfm?ty=pbdetail&iid=4821

[8] Computer Research News. The 10 Biggest Data Breaches of 2015 (So Far). (2015). Retrieved from http://www.crn.com/slide-shows/security/300077563/the-10-biggest-data-breaches-of-2015-so-far.htm

[9] The Ponemon Institute. Criminal Attacks are Now the Leading Cause of Data Breach in Healthcare. ((2015). Retrieved from http://www.ponemon.org/news-2/66

[10] Space War. US Air Force Prepares for Cyber Warfare. (2006). Retrieved from http://www.spacewar.com/reports/US_Air_Force_Prepares_For_Cyber_Warfare_999.html

[11] US Joint Forces Command. The Joint Operating Environment. (2010). Retrieved from http://www.peakoil.net/files/JOE2010.pdf

[12] Greater Houston Regional Computer Forensic Laboratory. https://www.rcfl.gov/houston

[13] RCFL. Annual Report. (2012). Retrieved from http://www.rcfl.gov/annual-reports

[14] Cooper, P.A. (2005) Speciation in the Computing Sciences: Digital Forensics as an Emerging Academic Discipline. Proceedings of IPSI 2005 ISBN 86-7466-117-3.

[15]. National Computer Forensics Institute. Retrieved from https://www.ncfi.usss.gov/ncfi/

[16] Kessler, G.C. & Haggerty, D. (2008) Pedagogy Overview of a Graduate Program in Digital Investigation Management. Proceedings of the 41st Hawaii International Conference on System Sciences

[17] Yasinsac, A., Erbacher, R., Marks, D., Pollitt, M., and Sommer, P. Computer Forensics Education. IEEE Security & Privacy, July/August 2003, 15-23

[18] Texas Workforce Commission. State of Texas Information and Computing Technology Cluster. (2005). Retrieved from http://www.texasindustryprofiles.com/PDF/twcClusterReports/TexasITCluster.pdf

[19] Interlink. 2015-2020 InterLink Targeted High Skill/High Demand Occupations. (2015). Retrieved from http://www.interlink-ntx.org/pdfs/targetedlist.pdf

[20] The National Academies Press. Professionalizing the Nation's Cyber Security Workforce: Criteria for Decision-Making (2013). Retrieved from http://www.nap.edu/catalog.php?record_id=18446

[21] The Chronicle of Higher Education. https://chroniclevitae.com/job_search/new?cid=chenav. Accessed 2/16/2015.

[22] Digital Forensics Association. http://www.digitalforensicsassociation.org/

[23] The Accreditation Board for Engineering and Technology. ABET/CAC. http://www.abet.org/cac-membership/

[24] The Association for Computing Machinery. http://www.acm.org

[25] Computer Research Associates. The Taulbee Report 2013. Retrieved from http://cra.org/govaffairs/blog/2013/03/taulbeereport/

[26] High Tech Crime Investigator's Association. http://www.htcia.org/

[27] National White Collar Crime Center. http://www.nw3c.org/

COSTS TO THE INSTITUTION OF THE PROPSED PROGRAM

COSTS TO THE INSTITUTION OF THE PROGRAM/ADMINISTRATIVE CHANGE

Note: Use this chart to indicate the dollar costs to the institution that are anticipated from the change requested.

Cost Category	Cost Sub-Category	1st Year	2nd Year	3rd Year	4th Year	5th Year	TOTALS
Faculty Salaries[1]	(New)	$112,200	$207,405	$212,590	$287,205	$310,305	$1,129,705
	(Reallocated)						
Program Administration [2]	(New)						
	(Reassignments)	$32,160	$34,764	$37,433	$40,169	$42,973	$187,499
Graduate Assistants	(New)	$118,000	$259,600	$424,800	$590,000	$755,200	$2,147,600
	(Reallocated)						
Clerical/Staff [3]	(New)	$39,917	$40,914	$41,937	$42,986	$44,064	$209,818
	(Reallocated)						
Supplies & Materials		$3,000	$3,000	$3,000	$3,000	$3,000	$15,000
Library & IT Resources*		$3,000	$3,000	$3,000	$3,000	$3,000	$15,000
Equipment		$3,000	$12,000	$14,000	$14,000	$14,000	$57,000
Facilities		$0	$0	$0	$0	$0	$0
Other (Identify)[5]		$32,000	$40,000	$48,000	$56,000	$65,000	$241,000
TOTALS		$198,917	$600,683	$784,760	$1,036,360	$1.237,542	$4,002,622

Explanations: Explanations:

1. Faculty Salaries.
   The Faculty Availability Table indicates the need for 3 TBN faculty members. One position is an existing open position and scheduled to be filled fall 2015. The remaining two positions represent additional required resources. Estimated starting salaries for doctoral level faculty is $85,000 plus 32% benefits. These new positions will be appointed during years 2 and 3 of the program. Adjustment estimate of merit increases = 2.5% are included representing historic merit adjustments.

Students within the program can receive graduate assistant positions. ($20,000 plus 18% benefits). In each cohort, two students will be assigned teaching support roles, the remaining students will be assigned research assistant roles. The teaching assistantships will provide out of classroom support during year 2, and then be used to provide undergraduate service course coverage to compensate the use of core faculty involvement in the program. The research assistantships will provide research support for core and support faculty through the Center of Excellence in Digital Forensics.

2. Program Administration
The department chair will be responsible for program administration. The administration will be absorbed into the department chair's existing responsibilities. The department will appoint an assistant chair to support existing departmental administration. New costs to the University include 25% release ($10,000) during the spring semesters, 50% summer support ($13,000), and an annual stipend of $1,800. Calculations include 32% benefits. (Annual changes in salary reflect historic changes (2.5% per year).

3. Clerical Staff
A new secretary (Administrative Assistant II) will be hired for the proposed Program ($30,240 + 32% benefits=$38,707).

4. $25,000 to support internship and other doctoral student travel beginning summer of year 1.
Scholarship funds to be allocated on a competitive basis.

ANTICIPATED SOURCES OF FUNDING

Note: Use this table to indicate the dollar amounts anticipated from various sources to cover any and all new costs to the institution as a result of the proposed doctoral program. Use the Non-Formula Sources of Funding form to specify as completely as possible each non-general revenue source.

Funding Category	1st Year	2nd Year	3rd Year	4th Year	5th Year	TOTALS
I. Formula Income*			$274,127	$274,127	$709,997	$1,258,251
II. Other State Funding	$16,758	$59,985	$382,799	$436,709	$901,668	$1,797,919
III. Reallocation of Existing Resources	$140,341	$344,187	$361,828	$507,851	$617,163	$2,371,124
IV. Federal Funding (In-hand only)						
V. Other Funding						
TOTALS	$157,099	$404,172	$1,028,754	$1,218,687	$2,228,828	$5,027,540

*Use the Formula Funding Calculation Tool on the Coordinating Board web site to estimate income from the State. See also the *Guidelines for Institutions Submitting Proposals for New Doctoral Programs* document found on the Coordinating Board website for additional information.

NON-FORMULA SOURCES OF FUNDING

Note: Use this table to specify as completely as possible each of the non-formula funding sources for the dollar amounts listed on the Anticipated Sources of Funding form.

Funding Category	Non-Formula Funding Sources
II. Other State Funding	**#1Other State Funding includes Tuition ($50/SCH), Designated Tuition ($121/SCH), and Graduate tuition ($50/SCH)**
	#2
III. Reallocation of Existing Resources	**#1 Cost of faculty members assigned to the program. Salary + 32% benefits multiplied by the percentage of time allocated to teaching in the program.**
	#2
IV. Federal Funding	**#1**
	#2
V. Other Funding	**#1**
	#2

H. Institutional and Board of Regents Signature Page for Board Consideration

1. **Adequacy of Funding** – The chief executive officer shall sign the following statement:

   I certify that the institution has adequate funds to cover the costs of the new program. Furthermore, the new program will not reduce the effectiveness or quality of existing programs at the institution.

   Chief Executive Officer _____ Date 5-6-16

2. **Reimbursement of Consultant Costs** – The chief executive officer shall sign the following statement:

   I understand that the doctoral proposal process includes the use of external consultants. In the event that one or more consultants are contracted to review a doctoral proposal put forward by my institution, I understand that my institution will be required to reimburse the Texas Higher Education Coordinating Board for costs associated with the use of such consultants. By signing, I agree on behalf of my institution to provide reimbursement for consultant costs.

   Provost/Chief Executive Officer _____ Date 5-6-16

3. **Board of Regents Certification of Criteria for Board Consideration** -- The Board of Regents or designee must certify that the new program has been approved by the Board of Regents and meets the fourteen criteria under Texas Administrative Code (TAC) Section 5.46.

   On behalf of the Board of Regents, I certify that the new program meets the fourteen criteria specified under TAC Section 5.46 and has been approved by the Board of Regents.

   Board of Regents (Designee) _____ Date _____

H. Board of Regents
Signature Page for Commissioner Consideration

4. **Board of Regents Certification of Criteria for Commissioner or Assistant Commissioner Consideration** – Typically doctoral programs are approved by the Board, supported with a recommendation for approval by the Commissioner. Under very limited circumstance a program may be approved by the Commissioner. In this case only, the Board of Regents or designee must certify that the new program meets the criteria under Texas Administrative Code (TAC) Section 5.50 (b) and (c).

TAC §5.50(b) The program:

(1) has a curriculum, faculty, resources, support services, and other components of a degree program that are comparable to those of high quality programs in the same or similar disciplines at other institutions;
(2) has sufficient clinical or in-service sites, if applicable, to support the program;
(3) is consistent with the standards of the Commission of Colleges of the Southern Association of Colleges and Schools and, if applicable, with the standards or discipline-specific accrediting agencies and licensing agencies;
(4) attracts students on a long-term basis and produce graduates who would have opportunities for employment; or the program is appropriate for the development of a well-rounded array of basic baccalaureate degree programs at the institution;
(5) does not unnecessarily duplicate existing programs at other institutions;
(6) does not be dependent on future Special Item funding;
(7) has new five-year costs that would not exceed $2 million.

TAC §5.50 (c)The program:

(1-2) is in a closely related discipline to an already existing doctoral program(s) which is productive and of high quality;
(3) has core faculty that are already active and productive in an existing doctoral program;
(4) has a strong link with workforce needs or the economic development of the state; and
(5) the institution has notified Texas public institutions that offer the proposed program or a related program and resolved any objections.

On behalf of the Board of Regents, I certify that the new program meets the criteria specified under TAC Section 5.50 (b and c) and has been approved by the Board of Regents.

_____ _____

Board of Regents (Designee) Date