SANS Technology Institute

SANS Technology Institute

11200 Rockville Pike, Ste. 200
North Bethesda, MD, 20851
(301) 241-7665 | info@sans.edu

DAVID HOELZER
Dean of Faculty

JOHANNES ULLRICH
Dean of Research

TIM MEDIN
MSISE Program Director

ALAN PALLER
President

ERIC PATTERSON
Executive Director

BETSY MARCHANT
Assistant Director

Wednesday, May 20, 2020

James D. Fielder, Jr., Ph.D.
Secretary of Higher Education
Maryland Higher Education Commission
Nancy S. Grasmick Building, 10th Floor
6 North Liberty Street
Baltimore, MD 21201

Dear Dr. Fielder,

I am pleased to submit, on behalf of the SANS Technology Institute, the attached proposal for substantial modification to our existing Master's of Science in Information Security Engineering.

I look forward to answering any questions you or your staff may have, or providing additional information as needed. I can be reached by cell phone at 301-520-2835.

Sincerely,

Alan Paller
President
SANS Technology Institute

MHEC
ENGAGE • INFORM • SUPPORT

Office Use Only: PP#

Cover Sheet for In-State Institutions
New Program or Substantial Modification to Existing Program

Institution Submitting Proposal	SANS Technology Institute

Each action below requires a separate proposal and cover sheet.

○ New Academic Program	● Substantial Change to a Degree Program
○ New Area of Concentration	○ Substantial Change to an Area of Concentration
○ New Degree Level Approval	○ Substantial Change to a Certificate Program
○ New Stand-Alone Certificate	○ Cooperative Degree Program
○ Off Campus Program	○ Offer Program at Regional Higher Education Center

Payment Submitted: ○ Yes ○ No	Payment Type: ○ R*STARS ○ Check	Payment Amount:	Date Submitted:

Department Proposing Program	Operations	
Degree Level and Degree Type	Graduate, Master's	
Title of Proposed Program	Masters of Science in Information Security Engineering (MSISE)	
Total Number of Credits	36	
Suggested Codes	HEGIS: 5199.00	CIP: 11.1003
Program Modality	● On-campus	○ Distance Education (*fully online*)
Program Resources	● Using Existing Resources	○ Requiring New Resources
Projected Implementation Date	● Fall ○ Spring	○ Summer Year: 2020
Provide Link to Most Recent Academic Catalog	URL: sans.edu/downloads/STI-Course-Catalog 2020	
Preferred Contact for this Proposal	Name: Betsy Marchant	
	Title: Assistant Director	
	Phone: (804) 519-6863	
	Email: bmarchant@sans.edu	
President/Chief Executive	Type Name: Alan Paller	
	Signature:	Date: 05/19/2020
	Date of Approval/Endorsement by Governing Board:	12/13/2019

Revised 4/2020

Proposal for a Substantial Modification to an Existing Degree Program: Master's of Science in Information Security Engineering

SANS Technology Institute
May 2020

Table of Contents

TABLE OF CONTENTS 2

CENTRALITY TO INSTITUTIONAL MISSION AND PLANNING PRIORITIES 4

PROGRAM DESCRIPTION 4
RELATION TO MISSION, VISION, AND STRATEGIC GOALS OF STI 4
SUMMARY OF KEY CHANGED ELEMENTS 5

CRITICAL AND COMPELLING REGIONAL OR STATEWIDE NEED AS IDENTIFIED IN THE STATE PLAN 7

DEMAND AND NEED FOR PROGRAM 7
RELEVANCE TO HISTORICALLY BLACK INSTITUTIONS 7
ALIGNMENT WITH MARYLAND STATE PLAN FOR POSTSECONDARY EDUCATION 7

QUANTIFIABLE AND RELIABLE EVIDENCE AND DOCUMENTATION OF MARKET SUPPLY AND DEMAND IN THE REGION AND STATE 9

REASONABLENESS OF PROGRAM DUPLICATION 10

RELEVANCE TO HIGH-DEMAND PROGRAMS AT HISTORICALLY BLACK INSTITUTIONS (HBIS) 10

RELEVANCE TO THE IDENTITY OF HISTORICALLY BLACK INSTITUTIONS (HBIS) 10

ADEQUACY OF CURRICULUM DESIGN, PROGRAM MODALITY, AND RELATED LEARNING OUTCOMES 11

ESTABLISHMENT OF PROGRAM AND FACULTY 11
EDUCATIONAL OBJECTIVES AND INTENDED STUDENT LEARNING OUTCOMES 12
COURSE DESCRIPTIONS 12
FOCUS AREAS 20
GENERAL EDUCATION REQUIREMENTS 20
SPECIALIZED ACCREDITATION/CERTIFICATION REQUIREMENTS 20
CONTRACT WITH ANOTHER INSTITUTION OR NON-COLLEGIATE ORGANIZATION 20

ADEQUACY OF ARTICULATION 21

ADEQUACY OF FACULTY RESOURCES 21

ADEQUACY OF LIBRARY RESOURCES 26

ADEQUACY OF PHYSICAL FACILITIES, INFRASTRUCTURE AND INSTRUCTIONAL EQUIPMENT 27

ADEQUACY OF FINANCIAL RESOURCES WITH DOCUMENTATION 28

TABLES 28
FINANCIAL DATA NARRATIVE 29

ADEQUACY OF PROVISIONS FOR EVALUATION OF PROGRAM 31

CONSISTENCY WITH THE STATE’S MINORITY STUDENT ACHIEVEMENT GOALS 32

RELATIONSHIP TO LOW PRODUCTIVITY PROGRAMS IDENTIFIED BY THE COMMISSION 32

ADEQUACY OF DISTANCE EDUCATION PROGRAMS 33

APPENDIX 1. CONTRACTS WITH RELATED ENTITIES 41

Centrality to Institutional Mission and Planning Priorities

Program Description

The MSISE is a 36-credit hour, graduate level program comprised of an integrated mix of technical and management courses which include faculty instruction, research, projects, assessments, and simulations that progressively develop the capabilities required by a technically proficient leader in information security engineering. It was initially established and approved by the Maryland Higher Education Commission in 2005. The program is designed to be completed in three years by full-time, working professionals who have at least a year or more of experience in information technology, information security, or audit. It is not meant as an introduction to the information security field, but as a program that will advance the capabilities and careers of individuals who are already employed in the field. Students are often supported in the program by their employer and most expect to stay employed by their current employer after graduation. Most of the courses are offered in multiple formats, allowing an individual student the option to take much of the program at-a-distance using one or more of our online modalities, or, conversely, to take program in-classroom at our residential institute events that are comprised of 36-47 hours of intensive instruction by our faculty over five to six days.

There are 'focus areas' available, whereby students may make elective choices that coincide with the areas of Cyber Defense Operations, Penetration Testing and Ethical Hacking, Digital Forensics and Incident Response, Security Management and Policy, and Industrial Control Systems.

Relation to Mission, Vision, and Strategic Goals of STI

The MSISE program is directly aligned with the formal mission of the SANS Technology Institute:

> The SANS Technology Institute develops technically-skilled professionals and leaders who strengthen global information security through innovative and flexible approaches to learning. We prepare our students to master advanced practices through experiential and project-based learning which is delivered by faculty who are top scholar-practitioners in the industry, and our graduates implement and execute state-of-the-art cybersecurity.

The formal Vision of the SANS Technology Institute is:

> The SANS Technology Institute aspires to be the preeminent institution translating contemporary information security practice, scholarship, and research into effective educational experiences.

In so doing, STI will:

> 1. Enable private and public sector enterprises of the United States and its allies to preserve social order and protect their economic rights and military capabilities in the face of cyber attacks;
> 2. Provide the national defense establishment, critical industries, businesses and government agencies with information security engineers and managers who have the most current and critical knowledge and skills needed to respond effectively to the evolving cyber attack landscape; and,
> 3. Perform leading-edge research that continually identifies current best practice and enhances the state of the art in the practice of information security.

The MSISE program seeks to develop security practitioners who excel as technical leaders in their organizations. The program is designed to ensure that each student achieves knowledge of the core, foundational domains of information security, plus allows them elective choices to develop either concentrations in particular domains, or add to the breadth of their expertise by exploring a mixed set of topics beyond the core areas. The MSISE program prepares students to weave deep technical expertise into the design of effective cybersecurity. It also provides them with the communications skills and knowledge to gain proactive support for security enhancements from (1) higher-level management, (2) other peer organizational leaders and staff who must cooperate in adopting the enhancements, and (3) technical team members who must build and deploy those enhancements. The MSISE program, therefore, fits directly within the focused mission of the SANS Technology Institute in developing technical experts who lead information security technology programs.

The SANS Technology Institute is focused on developing information security leaders who have a combination of deep technical skills, knowledge of effective practice, and leadership competencies that will allow them to design, deploy, and manage effective enterprise information security environments. Every major element of the college—from admissions to courses, student advising, research, and public service—is closely aligned with that mission. Given the small number of programs offered at STI, the success of the MSISE program remains a key strategic goal for STI and is further outlined in our strategic plan.

STI updated the institutional strategic plan in 2017, focusing on the next 5 years, which we believe are critical for the continuing success of the institution. As a result the following strategic goals were established:

1. Materially Increase the Number of Graduates Prepared to Lead Cybersecurity Teams, Programs, and Efforts.

2. Modify Academic Program Design & Delivery to Maximize Graduates with Leadership Capabilities

3. Align Organizational Design and Processes to Optimize Support of the Student Experience

The MSISE curriculum is a driving factor in recruiting, educating and graduating information security professionals with a strong technical knowledge and skill set, therefore, the success of the program is critical to the success of the institute.

Summary of Key Changed Elements

This proposal of substantial modification is the result of a comprehensive program review of the Master of Science in Information Security Engineering (MSISE) degree program in 2019, which assessed (1) the content, balance, coherence, and rigor of the MSISE curriculum, (2) the alignment of student performance and outcomes with the program's learning objectives and with the STI mission, and (3) the alignment of the program's learning outcomes with employers' needs and expectations.

Largely, the proposed changes with regards to the concepts, content, or course level learning outcomes are minimal. However, by replacing one technical course, adding management instructional content, changing course numbers for versioning, and rebalancing of the credit load within the program, we will meet the 33% changed threshold in which necessary to submit a formal change proposal.

Current graduation requirements

(with planned changes outlined in the comments field)

Required Course	Course Name	Credits	Comments
ISE 5101	Security Essentials	3	
ISE 5201	Hacking Techniques & Incident Response	3	
ISE 5300	Building Security Awareness	1	
ISE 5401	Advanced Network Intrusion Detection & Analysis	3	
~~ISE 5501~~	~~Technical Research & Communication Practicum~~	~~3~~	This course is redundant (same as ISE 5901) and will be removed from the curriculum.
~~ISE 5600~~	~~IT Security Leadership Competencies~~	~~1~~	This course will include more instructional

			content, an exam, and will be 3 credits. It will be renamed ISE 5601.
~~ISE 5700~~	~~Situational Response Practicum~~	1	This course will have added instructional content and will be renamed ISE 5701.
ISE 5800	IT Security Project Management	3	
ISE 5901	Advanced Technical Research & Communication Practicum	3	
~~ISE 6001~~	~~Standards Based Implementation of Security~~	~~3~~	This course will be removed from the curriculum and replaced with ISE 6255.
~~ISE 6100~~	~~Security Project Practicum~~	~~1~~	This course will have added instructional content and will be renamed ISE 6101.
ISE 6300	NetWars Continuous Practicum	1	
ISE 6999	3 Elective Courses	9	
~~ISE 7000~~	~~MSISE Capstone~~	1	This course will be re-imagined as 2 separate program assessments, one at mid-program and the second as a capstone, each earning 1 credit – ISE 6200 and ISE 6901.

Proposed Graduation Requirements

Required Course	Course Name	Credits
ISE 5101	Security Essentials	3
ISE 5201	Hacking Techniques & Incident Response	3
ISE 5601	IT Security Leadership Competencies	3
ISE 6255	Defensible Security Architecture & Engineering	3
ISE 5300	Building Security Awareness	1
ISE 5401	Advanced Network Intrusion Detection & Analysis	3
ISE 5701	Situational Response Practicum	1
ISE 6200	Technical Research & Communication Practicum	1
ISE 5800	IT Security Project Management	3
ISE 5901	Advanced Technical Research & Communication Practicum	3
ISE 6101	Security Project Practicum	1
ISE 6300	NetWars Continuous Practicum	1
ISE 6999	3 Elective Courses	9
ISE 6901	MSISE Capstone	1

Critical and Compelling Regional or Statewide Need as Identified in the State Plan

Demand and Need for Program

Cybersecurity is a national priority and critical to the well-being of organizations. As technology becomes increasingly sophisticated, demand for an experienced and qualified workforce is essential. The MSISE program is directly supportive of the development of professionals with the skills and capabilities to design, implement, and manage the protection of information assets that are central to the advancement and evolution of knowledge in the information age.

Cyberseek, a website created by the National Institute of Standards and Technology (NIST), indicates that there are 504,316 cybersecurity job openings nationally. CyberSeek states that the supply of cybersecurity workers nationally is "very low" relative to the demand. In Maryland alone, CyberSeek shows that there are 20,516 job openings and 2,550 of those openings that specifically request GIAC certifications which are obtained as a degree requirement of the MSISE program. These data indicate a high demand not just for cybersecurity workers, but especially for those who have proven, by holding GIAC certifications, that they have the skills to do the job. In combining CyberSeek data with employment projections from the Maryland Department of Labor Licensing and Regulation (DLLR) to estimate the continuing and growing demand for the STI MSISE program in Maryland and in the region.

Cybersecurity jobs are already an important part of Maryland's economy, comprising the second highest concentration of professional and technical workers among all fifty states. With the increasing recognition of the vulnerability of critical public and private networks and the need to better protect those networks against constantly evolving threats, it is reasonable to expect that, in conjunction with the State Plan, Maryland will continue to attract additional information security workers and separating military veterans who wish to enter into this challenging field. This growth will call for educated technical leaders with diverse skillsets and the ability to implement, develop, integrate, orchestrate, and lead cybersecurity operations.

Relevance to Historically Black Institutions

This program proposal will have no impact on the uniqueness and institutional identity of mission of HBIs, as it does not represent a net change in the number or kind of offerings in graduate cybersecurity education within Maryland.

Alignment with Maryland State Plan for Postsecondary Education

Increase student success with less debt

This program will address the State Plan's goals to increase student success with less debt. Approximately 33% of our students fully fund their studies by way of employer tuition reimbursement, while another 43% utilize veteran education benefits.

Supporting veterans

Strategy 7 calls for special efforts to support veterans. Approximately 43% of our current study body is comprised of veterans, with nearly all of them using some combination of GI Bill benefits and employer tuition reimbursement to increase their knowledge and skills as they enter or further establish themselves in the civilian workforce.

Develop new partnerships between colleges and businesses to support workforce development and improve workforce readiness

The MSISE program makes substantial contributions to Maryland's goals by seeking to increase the number and quality of graduates who are desperately in demand in business and industry verticals across the state.

Cybersecurity jobs are already an important part of Maryland’s economy, comprising the second highest concentration of professional and technical workers among all fifty states. Yet, even with this standing, the demand for skilled and educated cybersecurity practitioners is outstripping the available supply. With more than 45,000 information security workers employed in Maryland, the state currently has more than 20,000 job openings in the field, with nearly 3,000 of those positions categorized as being in the “Oversee and Govern” domain according to the NICE Cybersecurity Workforce Framework.

Quantifiable and Reliable Evidence and Documentation of Market Supply and Demand in the Region and State

The MSISE program is focused on developing information security leaders who have a combination of deep technical skills, knowledge of effective practice, and leadership competencies that will allow them to design, deploy, and manage effective enterprise information security environments.

Cyberseek, a website created by the National Institute of Standards and Technology (NIST), indicates that there are 504,316 cybersecurity job openings nationally. CyberSeek states that the supply of cybersecurity workers nationally is “very low” relative to the demand. In Maryland alone, CyberSeek shows that there are 20,516 job openings and 2,550 of those openings that specifically request GIAC certifications which are obtained as a degree requirement of the MSISE program. These data indicate a high demand not just for cybersecurity workers, but especially for those who have proven, by holding GIAC certifications, that they have the skills to do the job. In combining CyberSeek data with employment projections from the Maryland Department of Labor Licensing and Regulation (DLLR) to estimate the continuing and growing demand for the STI MSISE program in Maryland and in the region.

Cybersecurity jobs are already an important part of Maryland’s economy, comprising the second highest concentration of professional and technical workers among all fifty states. With the increasing recognition of the vulnerability of critical public and private networks and the need to better protect those networks against constantly evolving threats, it is reasonable to expect that, in conjunction with the State Plan, Maryland will continue to attract additional information security workers and separating military veterans who wish to enter into this challenging field. This growth will call for educated technical leaders with diverse skillsets and the ability to implement, develop, integrate, orchestrate, and lead purple teams and operations.

With the strategic goal set in 2017 to “Materially increase the number of graduates prepared to lead cybersecurity teams, programs, and efforts,” STI expects to have 200 MSISE graduates per year by the 2022.

Reasonableness of Program Duplication

This proposal for a “Substantial Modification” to the SANS Technology Institute’s MSISE program does not alter the number or nature of existing programs related to information security engineering in Maryland, nor how our program relates to those programs. As this substantial modification mainly seeks to establish changes to program organization by way of course numbering and naming, and which incorporates only a marginal change of program learning outcomes, academic requirements, or course content, we do not feel that anything provided in this substantial modification impacts the prior determinations by MHEC regarding program duplication.

Relevance to High-demand Programs at Historically Black Institutions (HBIs)

No HBI offers a comparable credential.

Relevance to the identity of Historically Black Institutions (HBIs)

This program proposal will have no impact on the uniqueness and institutional identity of mission of HBIs, as it does not represent a net change in the number or kind of offerings in graduate cybersecurity education within Maryland.

Adequacy of Curriculum Design, Program Modality, and Related Learning Outcomes

Establishment of Program and Faculty

The MSISE is a 36-credit hour, graduate level program comprised of an integrated mix of technical and management courses which include faculty instruction, research, projects, assessments, and simulations that progressively develop the capabilities required by a technically proficient leader in information security engineering. It was initially established and approved by the Maryland Higher Education Commission in 2005.

The MSISE program is overseen by a faculty committee that includes the following individuals:

Dr. Johannes Ullrich
Johannes is Dean of Research at STI and also created and manages the SANS Internet Storm Center (ISC) and the GIAC research paper program. In 2000, he founded DShield.org, which is now the data collection engine behind the ISC. His work with the ISC has been widely recognized, and in 2004, Network World named him one of the 50 most powerful people in the networking industry. Johannes holds a PhD in physics from SUNY Albany. His daily podcast, listened to by more than 10,000 professionals, summarizes current security news in a concise format.

David Hoelzer
David is the Dean of Faculty at STI. He is the author of more than twenty days of SANS courseware. He is an expert in a variety of information security fields, having served in most major roles in the IT and security industries over the past twenty-five years. Recently, David was called upon to serve as an expert witness for the Consumer Financial Protection Bureau in a landmark case regarding information security governance within corporations in the financial sector and has previously served as an expert for the Federal Trade Commission for GLBA Privacy Rule litigation and other matters. David has been highly involved in governance at SANS Technology Institute, serving as a member of the Curriculum Committee, Long Range Planning Committee, GIAC Ethics Board, and as Dean of Faculty. As a SANS instructor, David has trained security professionals from organizations including NSA, DHHS, Fortune 500 security engineers and managers, various Department of Defense sites, national laboratories, and many colleges and universities. Outside of SANS, David is a research fellow in the Center for Cybermedia Research, a research fellow for the Identity Theft and Financial Fraud Research Operations Center (ITFF/ROC), an adjunct research associate of the UNLV Cybermedia Research Lab, a research fellow with the Internet Forensics Lab, and an adjunct lecturer in the UNLV School of Informatics. David has written and contributed to more than 15 peer reviewed books, publications, and journal articles. Currently, David serves as the principal examiner and director of research for Enclave Forensics, a New York/Las Vegas based incident response and forensics company. He also serves as the chief information security officer for Cyber-Defense, an open-source security software solution provider. In the past, David served as the director of the GIAC Certification program, bringing the GIAC Security Expert certification to life. David holds a BS in IT and an MS in Computer Science, having spent time either attending or consulting for Stony Brook University, Binghamton University, and American Intercontinental University.

Tim Medin
Tim is STI's Director for the MSISE program and is a course author. He is the founder and Principal Consultant at Red Siege, a company focused on adversary emulation and penetration testing. Through the course of his career, Tim has performed penetration tests on a wide range of organizations and technologies. He gained information security experience in a variety of industries including previous positions in control systems, higher education, financial services, and manufacturing. Tim is an experienced international speaker, having presented to an organizations around the world. Tim is also the

creator of the Kerberoasting, a technique to extract kerberos tickets in order to offline attack the password of enterprise service accounts. Tim earned his MBA through the University of Texas.

Educational Objectives and Intended Student Learning Outcomes

The Master of Science in Information Security Engineering (MSISE) degree program prepares student to be the architects, designers, and lead builders of information security for an enterprise, defined here as an organization of sufficient size and complexity to have a dedicated information security team. Graduates will take on enterprise security technical leadership roles with titles such as Technical Director for Information Security, Senior Security Analyst, Senior Security Administrator, Information Systems Security Manager, Information Systems Security Officer, Information Security Manager, and Chief Information Security Officer. Graduates may also work as consultants who carry out the responsibilities of those positions, or who advise organizations on information security engineering issues. The MSISE program is designed to provide a sound theoretical framework delivered through a practitioner lens, but also to ensure that the graduate is capable of establishing adaptive security paradigms.

By the end of this program, graduates will be able to:

- Formulate and implement policies and solutions that demonstrate a thorough understanding of security foundations and practical applications of information technology.
- Demonstrate a solid foundation in information security strategies and apply their knowledge by assessing an information security situation and prescribing an appropriate security approach.
- Construct an information security approach that balances organizational needs with those of confidentiality, integrity and availability. Solutions require a comprehensive approach that aligns with policy, technology, and organizational education, training and awareness programs.
- Effectively communicate information security assessments, plans and actions for technical and nontechnical audiences/stakeholders.
- Identify emerging information security issues, utilize knowledge of information security theory to investigate causes and solutions, and delineate strategies guided by evolving information security research and theory.
- Analyze and design technical information security controls and safeguards, including system specific policies, network, and platform security countermeasures and access controls.
- Conduct threat assessments (offensive measures), appraise/prioritize vulnerabilities (defensive perspectives), and appraise technical risks for enterprise information assets/needs/requirements.
- Apply a standards-based approach to minimize risk through the implementation of the principles and applications of information security.
- Evaluate the appropriate security solutions required to design/build a security architecture, to include the integration of intrusion detection, defensive infrastructures, penetration testing, and vulnerability analysis.
- Formulate plans for adaptive detection of threats, including leading/oversight of intrusion/malware detection, incident response, forensics, reverse engineering, and e-discovery initiatives and actions.

Course Descriptions

ISE 5101: Security Essentials
SANS SEC 401 | GIAC GSEC | 3 Credit Hours | 90 Days

ISE 5101 establishes the foundations for designing, building, maintaining and assessing security functions at the end-user, network and enterprise levels of an organization. The faculty instruction, readings, lab exercises, and exam are coordinated to introduce and develop the core technical, management, and enterprise-level capabilities that will be developed throughout the rest of the certificate program.

ISE 5201: Hacker Tools, Techniques, Exploits, & Incident Handling
SANS SEC 504 | GIAC GCIH | 3 Credit Hours | 90 Days

By adopting the viewpoint of a hacker, ISE 5201 provides an in-depth focus into the critical activity of incident handling. Students are taught how to manage intrusions by first looking at the techniques used by attackers to exploit a system. Students learn responses to those techniques, which can be adopted within the framework of the incident handling process to handle attacks in an organized way. The faculty instruction, lab exercises and exam are coordinated to develop and test a student's ability to utilize the core capabilities required for incident handling.

ISE 5300: Building Security Awareness
SANS MGT 433 | SANS SSAP Exam | 1 Credit Hour | 45 Days

From phishing attacks and credential stuffing to lost devices or auto-complete in email, human risk has become the primary risk for most organizations. One of the most effective ways for an organization to manage its human risk is to build on their existing technical controls with a mature security awareness program. The program must go beyond just compliance and change organizational behaviors and ultimately, culture. In ISE/ISM 5300, you will learn the key concepts and skills to plan, maintain, and measure an effective security awareness program that makes an organization both more secure and compliant. Through a series of labs and exercises, you will develop your security awareness plan and also complete the SSAP exam.

ISE 5401: Intrusion Detection In-Depth
SANS SEC 503 | GIAC GCIA | 3 Credit Hours | 90 Days

ISE 5401 arms students with the core knowledge, tools, and techniques to detect and analyze network intrusions, building in breadth and depth for advanced packet and traffic analysis. Hands-on exercises supplement the course book material, allowing students to transfer the knowledge in their heads to their keyboards using the Packetrix VMware distribution. As the Packetrix name implies, the distribution contains many of the tricks of the trade to perform packet and traffic analysis.

ISE 5601: IT Security Planning, Policy, & Leadership
SANS MGT 514 | GIAC GSTRT | 3 Credit Hours | 90 Days

ISE 5601 covers the critical processes to be employed by technical leaders to develop the skills and techniques to select, train, equip, and develop a team into a single cohesive unit with defined roles that operate together in harmony toward team-objective accomplishment. Topics covered include: leadership development, coaching and training, employee involvement, conflict resolution, change management, vision development, motivation, communication skills, self-direction, brainstorming techniques, strategic planning and policy development, and the ten core leadership competencies.

ISE 5701 Situational Response Practicum
1 Credit Hour | 45 Days

The purpose of this course is for students to learn and be assessed on their ability to come together as a team, assess a situation, develop a response and prepare recommendations for decision to a C-Level audience within forty-five (45) days. You are put into a small group with other students and presented with an information security topic prompt. Your group then prepares a plan for researching and reporting on the assignment. Once the plan is prepared, the group executes the plan, adjusting as necessary, to develop a report of the research completed recommended actions.

ISE 6200: Core Comprehensive Exam
1 Credit Hour | 30 Days

The Core Comprehensive Exam determines if candidates have mastered the core technical skills required by top security consultants and individual practitioners. Through a series of exercises, students demonstrate their ability to integrate the knowledge, skills and techniques acquired in ISE 5101, ISE 5201, and ISE 5401 to address common challenges faced by technical leaders in the cybersecurity field.

ISE 5800: IT Security Project Management
SANS MGT 525 | GIAC GCPM | 3 Credit Hours | 90 Days

In ISE 5800 you will learn how to improve your project planning methodology and project task scheduling to get the most out of your critical IT resources. The course utilizes project case studies that highlight information technology services as deliverables. ISE 5800 follows the basic project management structure from the PMBOK® Guide 5th edition and also provides specific techniques for success with information assurance initiatives. All aspects of IT project management are covered - from initiating and planning projects through managing cost, time, and quality while your project is active, to completing, closing, and documenting as your project finishes.

ISE 5901 Advanced Technical Research & Communication Practicum
3 Credit Hours | 120 Days

ISE 5901 is an advanced graduate-level research and presentation course in which students will identify, investigate and analyze a problem. Students will write a whitepaper interpreting the data collected and making recommendations for action. The whitepaper will reflect original work towards a new practice, solution, tool, policy, or paradigm offering the potential for real impact in the field of information security.

Students will then convert written material to an oral presentation in order to inform a technical audience about the topic. Delivered via a webinar, students use material from their paper to build and deliver a 30-minute presentation and to then field questions. Students demonstrate a variety of presentation skills. Exemplary presentations may be selected to present at a live SANS event for further professional development.

ISE 6255: Defensible Security Architecture and Engineering
SANS SEC 530 | GIAC GDSA | 3 Credit Hours | 90 Days

Effective security requires a balance between detection, prevention, and response capabilities. Defensible Security Architecture and Engineering is designed to help students establish and maintain a holistic and layered approach to security. Students will learn the fundamentals of up-to-date defensible security architecture and how to engineer it, with a heavy focus on leveraging current infrastructure (and investment), including switches, routers, and firewalls. Students will learn how to reconfigure these devices to significantly improve their organization's prevention capabilities in the face of today's dynamic threat landscape. The course will also delve into the latest technologies and their capabilities, strengths, and weaknesses. Multiple hands-on labs conducted daily will reinforce key points in the course and provide actionable skills that students will be able to leverage as soon as they return to work.

ISE 6101 Security Project Practicum
1 Credit Hour | 30 Days

The purpose of this course is for students to learn and be assessed on their ability to come together as a team, assess a situation, demonstrate leadership, develop a response and prepare and present recommendations for a decision to a C-Level audience within 24-hours. This course builds on what you have learned in other courses and allows you to apply that knowledge. You are put into a small group with other students and presented with an information security topic prompt. Working as a group, you will analyze the situation, develop a technical response, and develop recommendations for an organizational response to the situation presented. Upon development of your recommended response, the group provides written and oral reports of recommendations for action to a mixed technical/non-technical audience of executives for decision.

ISE 6300 NetWars Continuous Practicum
1 Credit Hour | 60 Days

NetWars Continuous is an online training program that guides students through hands-on lessons to locate vulnerabilities, exploit diverse machines, and analyze systems. NetWars provides a forum to test and perfect cyber security skills in a manner that is legal and ethical. Students will face challenges derived from real-world environments and actual attacks that businesses, governments, and military organizations must deal with every day.

ISE 6901: MSISE Capstone
GIAC GSE Exam | 1 Credit Hour

The MSISE Capstone determines if candidates have mastered the wide variety of skills required by top security consultants and individual practitioners. Through a series of exercises, students demonstrate their ability to integrate the knowledge, skills and techniques acquired in individual courses into a cohesive toolset to address common challenges faced by technical leaders in the cybersecurity field.

Elective Courses (choose 3):

ISE 6215: Advanced Security Essentials
SANS SEC 501 | GIAC GCED | 3 Credit Hours | 90 Days

Students will learn how to design and build a secure network that can both prevent attacks and recover after a compromise. They will also learn how to retrofit an existing network to achieve the level of protection that is required. While prevention is important to learn, students will also learn how to detect the indications that the attack is in progress and stop it before significant harm is caused. Packet analysis and intrusion detection are at the core of this study. In the third module, students will learn about the variety of tests that can be run against an organization and how to perform effective penetration testing. To round out the defensive posture, students will learn the practice of identifying, analyzing, and responding effectively to attacks, including the identification of malware and steps that can be taken to prevent data loss.

ISE 6230: Securing Windows & PowerShell Automation
SANS SEC 505 | GIAC GCWN | 3 Credit Hours | 90 Days

ISE 6230 shows students how to secure servers, workstations and portable devices running Microsoft Windows. Windows is the most frequent target of hackers and advanced malware. While other courses focus on detection or remediation of a compromise after the fact, the aim of this course is to substantially reduce these compromises in the first place. For scalability and automation, this course includes many hands-on labs with Group Policy and PowerShell scripting. No prior scripting experience is required. Learning at least the basics of PowerShell is an essential skill for anyone who manages Windows servers or clients in an enterprise.

ISE 6235: Securing Linux/Unix
SANS SEC 506 | GIAC GCUX | 3 Credit Hours | 90 Days

ISE 6235 provides the specific technical education to enable students to secure Linux and Unix clients and infrastructure. This course is particularly valuable for students who are involved with sysadmins and network administrators, given the popularity of *nix tools in that space. The course covers various vulnerabilities and defenses and includes an introduction to forensic methods for *nix systems.

ISE 6240: Continuous Monitoring & Security Operations
SANS SEC 511 | GIAC GMON | 3 Credit Hours | 90 Days

A new proactive approach to security is needed to enhance the capabilities of organizations to detect threats that will inevitably slip through their defenses. ISE 6240 teaches this new proactive approach and strengthens student's skills to undertake that proactive approach. The Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Security Monitoring (CSM) taught in this course will help students best position their organization or Security Operations Center (SOC) to analyze threats and detect anomalies that could indicate cybercriminal behavior.

ISE 6245: SIEM with Tactical Analytics
SANS SEC 555 | GIAC GCDA | 3 Credit Hours | 90 Days

This course is designed to demystify the Security Information and Event Management (SIEM) architecture and process, by navigating the student through the steps of tailoring and deploying a SIEM to full Security Operations Center (SOC) integration.

ISE 6250: Purple Team Tactics & Kill Chain Defenses
SANS SEC 599 | GIAC GDAT | 3 Credit Hours | 90 Days

ISE 6250 leverages the purple team concept by bringing together red and blue teams for maximum effect. Recognizing that a prevent-only strategy is not sufficient, the course focuses on current attack strategies and how they can be effectively mitigated and detected using a Kill Chain structure. Throughout the course, the purple team principle will be maintained, where attack techniques are first explained in-depth, after which effective security controls are introduced and implemented.

ISE 6315: Web App Penetration Testing and Ethical Hacking
SANS SEC 542 | GIAC GWAPT | 3 Credit Hours | 90 Days

ISE 6315 is a highly technical information security course in offensive strategies where students learn the art of exploiting Web applications so they can find flaws in enterprise Web apps before they are otherwise discovered and exploited. Through detailed, hands-on exercises students learn the four-step process for Web application penetration testing. Students will inject SQL into back-end databases, learning how attackers exfiltrate sensitive data. They then utilize cross-site scripting attacks to dominate a target infrastructure in a unique hands-on laboratory environment. Finally, students explore various other Web app vulnerabilities in-depth with tried-and-true techniques for finding them using a structured testing regimen.

ISE 6320: Network Penetration Testing and Ethical Hacking
SANS SEC 560 | GIAC GPEN | 3 Credit Hours | 90 Days

ISE 6320 prepares students to conduct successful penetration testing and ethical hacking projects. The course starts with proper planning, scoping and recon, and then dives deep into scanning, target exploitation, password attacks, and wireless and web apps with detailed hands-on exercises and practical tips for doing the job safely and effectively. Students will participate in an intensive, hands-on Capture the Flag exercise, conducting a penetration test against a sample target organization.

ISE 6325: Mobile Device Security & Ethical Hacking
SANS SEC 575 | GIAC GMOB | 3 Credit Hours | 90 Days

ISE 6325 helps students resolve their organization's struggles with mobile device security by equipping then with the skills needed to design, deploy, operate, and assess a well-managed secure mobile environment. From practical policy development to network architecture design and deployment, and mobile code analysis to penetration testing and ethical hacking, this course teaches students to build the critical skills necessary to support the secure deployment and use of mobile phones and tablets in their organization.

ISE 6330: Wireless Penetration Testing & Ethical Hacking
SANS SEC 617 | GIAC GAWN | 3 Credit Hours | 90 Days

ISE 6330 takes an in-depth look at the security challenges of many different wireless technologies, exposing students to wireless security threats through the eyes of an attacker. Using readily available and custom-developed tools, students will navigate through the techniques attackers use to exploit WIFI networks, Bluetooth devices, and a variety of other wireless technologies. Using assessment and analysis techniques, this course will show students how to identify the threats that expose wireless technology and build on this knowledge to implement defensive techniques that can be used to protect wireless systems.

ISE 6350: Python for Penetration Testers
SANS SEC 573 | GIAC GPYC | 3 Credit Hours | 90 Days

The ISE 6350 course teaches student in the pen testing specialization, and other students who want to use the Python programming language, how to enhance their overall effectiveness during information security engagements. Students will learn how to apply core programming concepts and techniques learned in other courses through the Python programming language. The course teaches skills and techniques that can enhance an information security professional in penetration tests, security operations, and special projects. Students will create simple Python-based tools to interact with network traffic, create custom executables, test and interact with databases and websites, and parse logs or sets of data.

ISE 6360: Advanced Penetration Testing, Exploit Writing, & Ethical Hacking
SANS SEC 660 | GIAC GPEN | 3 Credit Hours | 90 Days

ISE 6360 builds upon ISE 6320 – Network Penetration Testing and Ethical Hacking. This advanced course introduces students to the most prominent and powerful attack vectors, allowing students to perform these attacks in a variety of hands-on scenarios. This course is an elective course in the Penetration Testing & Ethical Hacking certificate program, and an elective choice for the master's program in Information Security Engineering.

ISE 6420: Computer Forensic Investigations - Windows
SANS FOR 500 | GIAC GCFE | 3 Credit Hours | 90 Days

ISE 6420 Computer Forensic Investigations – Windows focuses on the critical knowledge of the Windows Operating System that every digital forensic analyst needs to investigate computer incidents successfully. Students learn how computer forensic analysts focus on collecting and analyzing data from computer systems to track user-based activity that can be used in internal investigations or civil/criminal litigation. The course covers the methodology of in-depth computer forensic examinations, digital investigative analysis, and media exploitation so each student will have complete qualifications to work as a computer forensic investigator helping to solve and fight crime.

ISE 6425: Advanced Digital Forensics, Incident Response, & Threat Hunting
SANS FOR 508 | GIAC GCFA | 3 Credit Hours | 90 Days

ISE 6425 teaches the necessary capabilities for forensic analysts and incident responders to identify and counter a wide range of threats within enterprise networks, including economic espionage, hacktivism, and financial crime syndicates. The course shows students how to work as digital forensic analysts and incident response team members to identify, contain, and remediate sophisticated threats-including nation-state sponsored Advanced Persistent Threats and financial crime syndicates. Students work in a hands-on lab developed from a real-world targeted attack on an enterprise network in order to learn how to identify what data might be stolen and by whom, how to contain a threat, and how to manage and counter an attack.

ISE 6440: Advanced Network Forensic Analysis
SANS FOR 572 | GIAC GNFA | 3 Credit Hours | 90 Days

ISE 6440 focuses on the most critical skills needed to mount efficient and effective post-incident response investigations. Moving beyond the host-focused experiences in ISE 6420 and ISE 6425, ISE 6440 covers the tools, technology, and processes required to integrate network evidence sources into investigations, covering high-level NetFlow analysis, low-level pcap exploration, and ancillary network log examination. Students will employ a wide range of open source and commercial tools, exploring real-world scenarios to help the student learn the underlying techniques and practices to best evaluate the most common types of network-based attacks.

ISE 6445: Cyber Threat Intelligence
SANS FOR 578 | GIAC GCTI | 3 Credit Hours | 90 Days

ISE 6445 will equip you, your security team, and your organization in the tactical, operational, and strategic level cyber threat intelligence skills and tradecraft required to better understand the evolving threat landscape and to accurately and effectively counter those threats. This course focuses on structured analysis in order to establish a solid foundation for any security skillset and to amplify existing skills.

ISE 6450: Advanced Smartphone Forensics
SANS FOR 585 | GIAC GASF | 3 Credit Hours | 90 Days

The focus of ISE 6450 is on teaching students how to perform forensic examinations on devices such as mobile phones and tablets. Students will add to their forensics skills with this course's focus on the advanced skills of mobile forensics, device file system analysis, mobile application behavior, event artifact analysis and the identification and analysis of mobile device malware. Students will learn how to detect, decode, decrypt, and correctly interpret evidence recovered from mobile devices. The course features a number of hands-on labs that allow students to analyze different datasets from smart devices and leverage the best forensic tools and custom scripts to learn how smartphone data hide and can be easily misinterpreted by forensic tools.

ISE 6460: Reverse-Engineering Malware
SANS FOR 610 | GIAC GREM | 3 Credit Hours | 90 Days

ISE 6460 teaches students how to examine and reverse engineer malicious programs – spyware, bots, Trojans, etc. – that target or run on Microsoft Windows, within browser environments such as JavaScript or Flash files, or within malicious document files (including Word and PDF). The course builds a strong foundation for reverse-engineering malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger and other tools. The malware analysis process taught in this class helps students understand how incident responders assess the severity and repercussions of a situation that involves malicious software and plan recovery steps. Students also experience how forensics investigators learn to understand key characteristics of malware discovered during the examination, including how to establish indicators of compromise (IOCs) for scoping and containing the incident.

ISE 6515: ICS/SCADA Security Essentials
SANS ICS 410 | GIAC GICSP | 3 Credit Hours | 90 Days

ISE 6515 ICS/SCADA Security Essentials is an introductory study of the information technology and operational technology roles that have converged in today’s industrial control system environments. This convergence has led to a greater need for a common understanding between the various groups who support or rely on these systems. Students in ISE 6515 will learn the language, the underlying theory, and the basic tools for industrial control system security in settings across a wide range of industry sectors and applications.

ISE 6520: ICS Active Defense and Incident Response
SANS ICS 515 | GIAC GRID | 3 Credit Hours | 90 Days

ISE 6520 will empower students to understand their networked industrial control system environment, monitor it for threats, perform incident response against identified threats, and learn from interactions with the adversary to enhance network security. The course uses a hands-on approach and real-world malware to break down cyber attacks on ICS from start to finish. Students will gain a practical and technical understanding of leveraging active defense concepts such as using threat intelligence, performing network security monitoring, and utilizing malware analysis and incident response to ensure the safety and reliability of operations.

ISE 6525: Essentials for NERC Critical Infrastructure Protection
SANS ICS 456 | GIAC GCIP | 3 Credit Hours | 90 Days

ISE 6525 empowers students with knowledge of the "what" and the "how" of the version 5/6 standards. The course addresses the role of FERC, NERC and the Regional Entities, provides multiple approaches for identifying and categorizing BES Cyber Systems and helps asset owners determine the requirements applicable to specific implementations. Additionally, the course covers implementation strategies for the version 5/6 requirements with a balanced practitioner approach to both cybersecurity benefits, as well as regulatory compliance.

ISE 6615: Defending Web Applications Security Essentials
SANS DEV 522 | GIAC GWEB | 3 Credit Hours | 90 Days

ISE 6615 covers the OWASP Top 10 and provides students with a better understanding of web application vulnerabilities, enabling them to properly defend organizational web assets. Mitigation strategies from an infrastructure, architecture, and coding perspective are discussed alongside real-world implementations that really work. The testing aspect of vulnerabilities is also covered so students can ensure their application is tested for the vulnerabilities discussed in class.

ISE 6650: Cloud Security and DevOps Automation
SANS SEC 540 | GIAC GCSA | 3 Credit Hours | 90 Days

ISE 6650 provides development, operations, and security professionals with a methodology to build and deliver secure infrastructure and software using DevOps and cloud services. Students will explore how the principles, practices, and tools of DevOps can improve the reliability, integrity, and security of on-premise and cloud-hosted applications. Starting with on-premise deployments, the first two days of the course examine the Secure DevOps methodology and its implementation using lessons from successful DevOps security programs. Students will gain hands-on experience using popular open-source tools to automate Configuration Management ("infrastructure as Code"), Continuous Integration (CI), Continuous Delivery (CD), containerization, micro-segmentation, automated compliance ("Compliance as Code"), and Continuous Monitoring. After laying the DevSecOps foundation, the final three days move DevOps workloads to the cloud, build secure cloud infrastructure, and deliver secure software.

ISE 6715: Auditing & Monitoring Networks, Perimeters, & Systems
SANS AUD 507 | GIAC GSNA | 3 Credit Hours | 90 Days

ISE 6715 is organized specifically to provide a risk driven method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high-level audit issues and general audit best practice, students have the opportunity to dive deep into the technical how to for determining the key controls that can be used to provide a level of assurance to an organization. Tips on how to repeatably verify these controls and techniques for continuous monitoring and automatic compliance validation are given from real world examples.

ISE 6720: Legal Issues in Data Security and Investigations
SANS LEG 523 | GIAC GLEG | 3 Credit Hours | 90 Days

ISE 6720 introduces students to the new laws on privacy, e-discovery, and data security so students can bridge the gap between the legal department and the IT department. It also provides students with skills in the analysis and use of contracts, policies, and records management procedures.

Focus Areas

Master's candidates may elect to focus their elective courses in a particular area. If choosing a focus area, the student must select the following elective courses:

Focus Area	**Available Elective Courses**
Cyber Defense Operations	*Choose 3 from:* ISE 6215, ISE 6230, ISE 6235, ISE 6240, ISE 6250
Penetration Testing	*Choose 3 from:* ISE 6315, ISE 6320, ISE 6325, ISE 6330, ISE 6350, ISE 6360
Incident Response	*Choose 3 from:* ISE 6420, ISE 6425, ISE 6440, ISE 6445, ISE 6450, ISE 6460
Security Management	ISE 6720, ISE 6715, and any other elective from the approved catalog
Industrial Control Systems	ISE 6515, ISE 6525, ISE 6520

General Education Requirements

General education requirements are not applicable to SANS Technology Institute MSISE program. Students are required to have completed a bachelor's degree before admittance.

Specialized Accreditation/Certification Requirements

No specialized accreditations or certifications are required for this program or its students.

Contract with Another Institution or Non-collegiate Organization

The modifications made to the MSISE program precipitating this Program Proposal neither include nor impact any changes to any relationship the SANS Technology Institute has with another institution or non-collegiate organization. Courses are authored and taught by members of the faculty of the SANS Technology Institute. Commensurate with the approval of the SANS Technology Institute as a degree-granting institution in the State of Maryland in 2005, and as reviewed and accredited by the Middle States Commission on Higher Education, the SANS Technology Institute will continue to engage the support services of its parent, the Escal Institute for Advanced Technologies (d/b/a/ SANS Institute) and its sister subsidiary, GIAC. The agreements are not designed specifically for the MSISE program, but as supporting structures for STI, these agreements support the delivery and management of this program. The MOUs have enabled all STI degree programs since STI was established and were most recently reviewed and approved during the Middle States accreditation team visit, to include review by MHEC representative Dr. Kiphart.

Prospective and Current Student Communications

MSISE program requirements and student services are found on our website at www.sans.edu. All marketing materials will be updated with the new version of the curriculum.

Once enrolled, new students attend orientation before registering for their first course. During orientation (outlined at https://www.sans.edu/students/orientation), students learn about modalities, faculty/student interaction, learning management systems, costs and payment policies, and academic support services available. As a final stage of orientation, students meet with their advisor to discuss course and degree requirements and any questions that the students have a result of completing orientation.

Adequacy of Articulation

As a master's degree program, STI's MSISE program does allow for the transfer or waiver of a limited amount of prior SANS coursework and/or GIAC examinations, as well as a small number of other recognized information security industry certifications. STI does not accept for transfer coursework from other academic programs. Thus, no articulation agreements currently exist and none are anticipated.

Adequacy of Faculty Resources

The STI faculty is comprised of and appointed from the 100+ individuals who have achieved the status of being "SANS Certified Instructors," an industry-recognized demarcation of technical achievement practiced in the field, superior teaching effectiveness and student engagement as exemplified in the classroom and online, and successful completion of a competitive development process that employs both student and peer-faculty feedback to prove that the instructors possess these qualities. Among the faculty are people who are called upon to investigate attacks on the U.S. government and our largest commercial enterprises, who are entrusted to teach practitioners of cybersecurity at the highest and most sensitive (classified) levels, and who through their professional practice and research advance our understanding of cyber threats and potential remediation, and then transmit that knowledge forward to our students and the larger community. Even beyond their superlative technical abilities, our faculty have skills as teachers that truly set them apart and allow them to impart sometimes dense technical lessons with enthusiasm, applicable real-world examples, and charismatic engagement. While a handful of faculty members serve in full-time teaching and research roles, most are scholar-practitioners who teach less than full-time for the school so that they can engage in the practice of cybersecurity, keep their skills advanced and current, and feed their experiences and learnings back into the courses and class discussions.

STI's current faculty leadership includes the following individuals:

Dr. Johannes Ullrich
Johannes is Dean of Research at STI and also created and manages the SANS Internet Storm Center (ISC) and the GIAC research paper program. In 2000, he founded DShield.org, which is now the data collection engine behind the ISC. His work with the ISC has been widely recognized, and in 2004, Network World named him one of the 50 most powerful people in the networking industry. Johannes holds a PhD in physics from SUNY Albany. His daily podcast, listened to by more than 10,000 professionals, summarizes current security news in a concise format.

David Hoelzer
David is the Dean of Faculty at STI. He is the author of more than twenty days of SANS courseware. He is an expert in a variety of information security fields, having served in most major roles in the IT and security industries over the past twenty-five years. Recently, David was called upon to serve as an expert witness for the Consumer Financial Protection Bureau in a landmark case regarding information security governance within corporations in the financial sector and has previously served as an expert for the Federal Trade Commission for GLBA Privacy Rule litigation and other matters. David has been highly involved in governance at SANS Technology Institute, serving as a member of the Curriculum Committee, Long Range Planning Committee, GIAC Ethics Board, and as Dean of Faculty. As a SANS instructor, David has trained security professionals from organizations including NSA, DHHS, Fortune 500 security engineers and managers, various Department of Defense sites, national laboratories, and many colleges and universities. Outside of SANS, David is a research fellow in the Center for Cybermedia Research, a research fellow for the Identity Theft and Financial Fraud Research Operations Center (ITFF/ROC), an adjunct research associate of the UNLV Cybermedia Research Lab, a research fellow with the Internet Forensics Lab, and an adjunct lecturer in the UNLV School of Informatics. David has written and contributed to more than 15 peer reviewed books, publications, and journal articles. Currently, David serves as the principal examiner and director of

research for Enclave Forensics, a New York/Las Vegas based incident response and forensics company. He also serves as the chief information security officer for Cyber-Defense, an open-source security software solution provider. In the past, David served as the director of the GIAC Certification program, bringing the GIAC Security Expert certification to life. David holds a BS in IT and an MS in Computer Science, having spent time either attending or consulting for Stony Brook University, Binghamton University, and American Intercontinental University.

Tim Medin
Tim is STI's Director for the MSISE program and is a course author. He is the founder and Principal Consultant at Red Siege, a company focused on adversary emulation and penetration testing. Through the course of his career, Tim has performed penetration tests on a wide range of organizations and technologies. He gained information security experience in a variety of industries including previous positions in control systems, higher education, financial services, and manufacturing. Tim is an experienced international speaker, having presented to organizations around the world. Tim is also the creator of the Kerberoasting, a technique to extract kerberos tickets in order to offline attack the password of enterprise service accounts. Tim earned his MBA through the University of Texas.

The full listing of STI faculty can be reviewed on our website at https://www.sans.edu/academics/faculty.

Faculty Recruitment and Development

One of the most serious responsibilities of the administration after student learning is the continued development and recruitment of qualified faculty. Especially since the institute is committed to using only Scholar/Practitioners of a Master Teacher caliber, continuous development and recruitment is critical to the sustainability of the college. To this end, the SANS Technology Institute and the affiliated SANS Institute partner for faculty development. The high-level roadmap for faculty development is illustrated in Figure 1.

To maintain the staffing levels required, the affiliated SANS Institute actively recruits individuals within the various communities of practice who demonstrate a high degree of mastery within a particular subject area as evidenced by achieving a high score on the ANSI accredited certification exam. Individuals who are willing to participate are then given additional coaching and training by a college faculty member and have the potential to eventually qualify as a Faculty member.

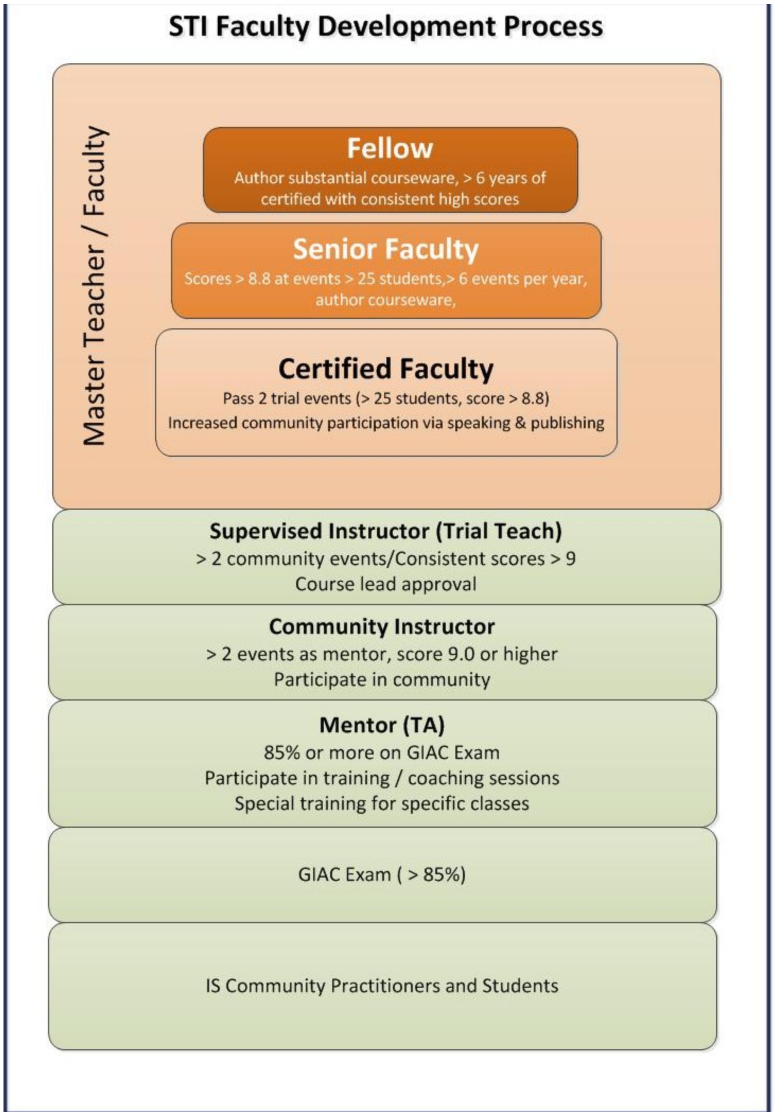
STI Faculty Development Process
Master Teacher / Faculty
Fellow
Author substantial courseware, > 6 years of certified with consistent high scores
Senior Faculty
Scores > 8.8 at events > 25 students,> 6 events per year, author courseware,
Certified Faculty
Pass 2 trial events (> 25 students, score > 8.8)
Increased community participation via speaking & publishing
Supervised Instructor (Trial Teach)
> 2 community events/Consistent scores > 9
Course lead approval
Community Instructor
> 2 events as mentor, score 9.0 or higher
Participate in community
Mentor (TA)
85% or more on GIAC Exam
Participate in training / coaching sessions
Special training for specific classes
GIAC Exam (> 85%)
IS Community Practitioners and Students

Figure 1 - Faculty Development Process

Mentor / TA

Individuals who demonstrate continued interest and ability are given the opportunity for coaching by a faculty member. Should he demonstrate willingness and an aptitude toward teaching, he will be given the opportunity to act as a “Mentor” for a particular course. The role of a mentor is to conduct a weekly recitation of material that students have prepared independently. His responsibility is to act as subject matter expert for this small group, providing an experience akin to a traditional Teaching Assistant role during a recitation.

Each Mentor is evaluated after each recitation by the students present. These evaluations are tabulated by an assessment analyst and forwarded to the staff of the affiliated SANS Institute for review and progress monitoring.

Community Instructor / TA

The success of a Mentor is measured by the outcome of student evaluations. Should a Mentor successfully complete two separate Mentoring experiences, he may qualify for an opportunity to participate at a smaller “Community” event hosted by the SANS Institute affiliate.

Prior to being invited to instruct at a Community event the candidate must first successfully pass a Murder Board. This is a live teaching simulation where the candidate must present a section of the course material to one or more of the college faculty. At least one of the faculty will have the role of challenging the potential instructor with difficult questions, unusual classroom control problems and other simulations to gauge both the subject matter mastery and the ability of the candidate to effectively control a classroom.

Trial Instructor / Supervised Instruction / TA

Community Instructors who, based on student evaluations, successfully teach at two separate Community engagements with the partner SANS Institute may qualify for an opportunity as a Trial Instructor. Qualification is contingent on approval from the Research Faculty responsible for the relevant course experience. Given that individuals at this strata are essentially candidates for Adjunct Faculty, a senior faculty member of the college will become engaged.

Trial Instructors are invited to work directly with a qualified senior member of the college faculty. Under the direction of the faculty member one hour segments of course material are selected for preparation and delivery by the trial instructor. Based on student evaluations and instructor observations, the trial instructor may be invited to present additional course hours.

Trial Instructors should expect to receive direct constructive feedback from the supervising faculty member. Trial Instructors are strongly encouraged to follow the recommendations of the supervising faculty member.

During the balance of the course experience, the Trial Instructor acts as a Teaching Assistant for the supervising faculty member. Trial Instructors are encouraged to pay close attention to how the faculty member delivers the course material, how the classroom is managed, how contact hours are managed and how student success and understanding is ensured.

Certified Instructor

Following two successful engagements as a Trial Instructor and based upon student evaluations and supervising faculty recommendation, a Trial Instructor may be promoted to Certified Instructor. At this point, the individual is qualified as an Adjunct Faculty member to teach courses within the college under the direction of the Professor of Practice, the Program Directors and the Research Faculty overseeing the particular courses being taught.

Certified Instructors, as Adjunct Faculty, are also expected to display the aspects of a Scholar/Practitioner as discussed on page **Error! Bookmark not defined.**. As a Certified Instructor/Adjunct Faculty it is also expected that the individual will maintain the high caliber of instructor required of a Master Teacher and, as such, will be subject to the same periodic assessment by the Program Directors and Professor of Practice.

Principal Instructor

This section previously wasn't included, not sure what needs to be said here.

Senior Instructor

Individuals who qualify as members of the faculty at the SANS Technology Institute are clearly outstanding. However, some faculty engage more deeply with the college and affiliated entities.

Faculty members who consistently achieve the highest evaluated ratings and who additionally have more than 240 course contact hours each year may qualify as Senior Instructors. Senior Instructors typically have additionally demonstrated significant leadership within the community of practice, perhaps through the development of course material used within the college or an affiliated entity.

Faculty Fellow

Those Senior Instructors who distinguish themselves through significant contributions to the community of practice and who have maintained a Senior Instructor designation for more than six years may be recommended to receive the designation of "Faculty Fellow."

While a Faculty Fellow does not receive any additional privileges within the college, it is expected that those receiving the Faculty Fellow distinction maintain a leadership position not only within his respective community of practice, but also among the faculty. These individuals should take a real interest in newly promoted faculty and strive to make them feel welcome in the faculty ranks. Faculty Fellows are also expected to be willing to come to the table when a mentor is needed for a fellow faculty member or potential faculty member who is struggling to meet or maintain his qualifications.

This designation is determined by the Academic and Student Affairs committee at one of its periodic meetings. Recommendations for Faculty Fellow are made by committee members. All discussions, recommendations, votes, etc. that pertain to Faculty Fellow recommendations are confidential.

Faculty Development Opportunities

Prospective faculty members who are progressing through the faculty development process, nearing certification as certified faculty members, have the opportunity to participate in a six-hour faculty development workshop. This workshop is overseen by a faculty fellow or curriculum lead. During the first three hours of the workshop, particular attention is given to the development of teaching skills, classroom management skills, keys for successful class preparation, and more through an interactive discussion with the instructor.

After the first three-hour discussion, prospective faculty members are given specific teaching assignments to prepare and are also assigned observation tasks to be completed over the next 18-24 hours. The second three-hour segment is dedicated to providing specific feedback to each participant on his or her own teaching style.

Faculty members may elect to attend the current iteration of this faculty development workshop at any point. Current faculty members may be asked to have limited participation in the presentation aspect in the second three hours depending upon enrollment constraints.

Faculty who participate in our OnDemand, vLive, and Simulcast distance learning modalities undergo specific training to help modify their style to this format. We engage a team of individuals to assist in online-specific methods to enable virtual student-faculty interactions, including (when a class is Simulcast to students) employing an assistant in the room who participates in the class on behalf of distance students by flagging the instructor's attention when questions are asked or issues are raised by virtual students.

Adequacy of Library Resources

The challenges of information security are constantly evolving, and excellence in performance demands continuous monitoring of changes in threats, technology, and practices. SANS conducts an extensive research program that helps STI students and alumni maintain their edge in security. The SANS Resource Center is a compilation of thousands of original research papers, security policies, and security notes, along with a wealth of unique network security data. Supplemented by an online research library subscription and other SANS information services, our current and future students have continuous access to the following list of primary resources:

- The SANS Information Security Reading Room, which contains more than 2,000 original research studies, not available from any other source, in 76 knowledge domains relevant to the study of information security. They are downloaded more than a million times each year.
- Free and unlimited access to EBSCO's "Computers and Applied Sciences (Complete)" database. EBCSO is the leading provider of online research databases, e-journals, magazine subscriptions, e-books, and discovery services of all kinds. This full-text database covers computing, technology and engineering disciplines, and contains 650 active full-text journals and magazines, 520 active full-text peer- reviewed journals, 320 active full-text peer-reviewed journals with no embargo, and 410 active full-text and indexed journals.
- The SANS Security Policy Collection, which contains model security policies developed by major corporations and government agencies. The collection contains about 35 policies and grows as new security issues arise and policy templates are needed.
- The SANS Technology Institute's Cyber Research page, which provides access to exemplary graduate-level research papers, group projects, and presentations that cover a wide variety of topics of practical and academic relevance that have real- world impact and often provide cutting-edge advancements to the field of cybersecurity knowledge.
- The SANS Top-20 V7, a consensus list of vulnerabilities that require immediate remediation. The list is the result of a process that brought together dozens of leading security experts.
- The SANS Newsletter Collection, which helps keep students up to date with the high- level perspective of the latest security news.
- The Security Glossary, which is among the largest glossaries of security terms available on the Internet. It was developed jointly by SANS and the National Security Agency and provides authoritative definitions of many of the specialized terms students will encounter.
- The SANS Collection of Frequently Asked Questions about Intrusion Detection, available at contains 118 authoritative discussions of the primary topics that arise when planning and implementing intrusion detection technologies. The collection is available at http://www.sans.org/security-resources/idfaq/.
- The SANS Internet Storm Center Handler Diaries and Archives, which contain contemporaneous analyses of new attacks that are discovered on the Internet. The archives constitute an extraordinary research asset because of the depth of the analysis and the currency of the topics covered. They also provide SANS students with access to raw data, summaries, and query facilities to analyze malicious Internet traffic records. This is a rich data source for advanced security research projects that analyze attack patterns and how fast worms and other attacks spread through the Internet.
- SANS Web Briefings held several times a month that feature SANS faculty and other security experts providing up-to-date web briefings for SANS alumni on new threats seen at the Internet Storm Center, ew techologies that are emerging, and analysis of security trends.

Adequacy of Physical Facilities, Infrastructure and Instructional Equipment

As a Proposal for Substantial Modification, there is no change in the physical facilities, infrastructure an instructional equipment required by the program. This program will continue to be offered in combinations of three online modalities and in residential institutes. More than 400 residential institutes are available to STI students each year with a cumulative capacity of more than 40,000 students. Each year the residential program expands by 10 to 20 institutes. Thus, the proposed program will easily be accommodated in the existing in-person training programs.

Similarly, the STI programs draw on SANS's online technology that currently serves more than 18,000 students each year and is not capacity-constrained.

Adequacy of Financial Resources with Documentation

Tables

Table 1: RESOURCES

Resource Categories	2020	2021	2022	2023	2024
1. Reallocated Funds	0	0	0	0	0
2. Tuition/Fee Revenue (c + g below)	4,400,000	5,500,000	6,875,000	8,250,000	9,625,000
a. Number of F/T Students	400	500	625	750	875
b. Annual Tuition/Fee Rate	11,000	11,000	11,000	11,000	11,000
c. Total F/T Revenue (a x b)	4,400,000	5,500,000	6,875,000	8,250,000	9,625,000
d. Number of P/T Students	0	0	0	0	0
e. Credit Hour Rate	0	0	0	0	0
f. Annual Credit Hour Rate	8	8	8	8	8
g. Total P/T Revenue (d x e x f)	0	0	0	0	0
3. Grants, Contracts & Other External Sources	0	0	0	0	0
4. Other Sources	0	0	0	0	0
TOTAL (Add 1 – 4)	4,400,000	5,500,000	6,875,000	8,250,000	9,625,000

Table 2: EXPENDITURES

Expenditure Categories	2020	2021	2022	2023	2024
1. Faculty (b + c below)	1,760,000	2,200,000	2,750,000	3,300,000	3,850,000
a. # Sections offered	N/A	N/A	N/A	N/A	N/A
b. Total Salary	1,056,000	1,320,000	1,650,000	1,980,000	2,310,000
c. Total Benefits	704,000	880,000	1,100,00	1,320,000	1,540,000
2. Admin. Staff (b + c below)	224,000	200,000	42000	42000	58800
a. # FTE	2.66	3.33	4.17	5	5.83
b. Total Salary	160,000	120,000	250,200	300,000	349,800
c. Total Benefits	64,000	80,000	100,080	120,000	139,920
3. Support Staff (b + c below)	0	0	0	0	0
a. # FTE	0	0	0	0	0
b. Total Salary	0	0	0	0	0
c. Total Benefits	0	0	0	0	0
4. Equipment	0	0	0	0	0
5. Library	0	0	0	0	0
6. New or Renovated Space	0	0	0	0	0
7. Other Expenses	50,000	58,000	66,000	74,000	82,000
TOTAL (Add 1 – 7)	2,034,000	2,450,000	4,816,280	5,774,000	6,761,720

Financial Data Narrative

Table 1: RESOURCES

Re-allocated Funds
N/A

Tuition and Fee Revenue
The tuition projection builds upon current student enrollment headcount and admissions trends. The projection also incorporates current retention data and average times to graduation.
Given current admissions trends, recent and ongoing investments in the marketing and admissions team and platforms, and our strategic goal MSISE graduates by 2021, we project that enrollment will increase as indicated in Table 1.

Grants and Contracts
N/A

Other Sources
N/A

Total Year
N/A

Table 2: EXPENDITURES

Faculty
MSISE students may receive instruction live in-classroom or online, depending on the course and their own choices. When they attend live in-classroom, they join a class already being taught by STI faculty to other students, to include non-STI students, and therefore MSISE students typically represent no more than a 5% - 10% increase in the total students in any given classroom. When they choose to take the course online, no additional faculty are required and, similar to live classes, MSISE students represent only a small fraction of those students being taught by the existing group of subject-matter experts and teaching assistants and at any given time. Therefore, we do not anticipate any increase in the number of faculty required to teach STI students, either live or online. While the cost associated with the faculty and subject-matter experts/teaching assistants who teach these students is embedded into the payments associated with the Memorandum of Understanding between STI and SANS we have, for the purpose of clarity, separated out estimated amounts for Faculty Salary and Compensation as per the indicated format for these tables.

Administrative and Support Staff
The STI graduate programs currently operate at a ratio of students to administrative staff ratio of 150:1.Average salary and benefit information is reflective of our current cost experience and market expectations.

Equipment, Library, New and/or Renovated Space
The MSISE program will not require any additional equipment, library facilities, or any new and/or renovated space. We have ample capacity in our existing facilities, residential institutes, online platform capacity, and offices.

Other Expenses

A core design element of the SANS Technology Institute are the Memoranda of Understanding signed with our parent, the SANS Institute, and a related entity, GIAC Corporation, that allow STI to select and pay for many costs on a variable, per-student basis. The financial projections assume the same mix of payments that STI incurs today per student, as recently reviewed by the Middle States evaluation team during our re-accreditation study.

Adequacy of Provisions for Evaluation of Program

Continuous, closed-loop evaluation has been the hallmark of STI programs since the school was established. STI employs a three-level evaluation program completely embedded in the curriculum. The 2018 Middle States Evaluation Team commended this evaluation methodology: “SANS Technology Institute should be commended for the fact that its curriculum automatically embraces learning outcomes and program outcomes.”

1. **Every day, in every STI class, every student is expected to complete an evaluation of the teaching effectiveness, the currency and value of the course material, and the quality of the labs, exercises, and other aspects of their learning experience.** Their forms are processed by an evaluation team and results are delivered by 6:30 the following morning to STI’s president and senior staff. The course faculty often reviews the forms the evening of the day they are completed. The evaluation team follows up on all strong concerns and, in several cases when a faculty member was clearly struggling, has replaced the teacher by noon the next day based on the evaluations. In addition, the evaluation team compiles and feeds course content suggestions or concerns to the course author for consideration or inclusion in the annual (or sometimes more frequent) course updates. Data on labs or other technology go to the appropriate teams for continuous or major product improvement. This evaluation system is also used in vLive and Simulcast distributed learning modalities. For On-Demand, the evaluation cycle is based on module completion rather than days, but the system functions identically and in fact responses are easier to process because entries are already in digital form when submitted.

2. **Evaluation of course-level student outcomes uses reliable measures of mastery** not subject to variability associated with individual faculty members’ understanding of the course outcomes. Each course has an associated examination that is recognized as a widely accepted and valued way to validate mastery of the course outcomes. For example, all MSISE students are required to complete a course in which they learn incident handling techniques, common attack techniques, and the most effective methods of stopping intruders using those attack techniques. The exam and certification associated with this course is called the Global Cybersecurity Incident Handler (GCIH) test and certification. The value of this exam is demonstrated by the fact that each year employers pay for more than 11,000 of their employees and job candidates to take this course and sit for the GCIH exam (pass rate of approximately 70%). The acceptance of the exam is validated by the U.S. Department of Defense (DoD) directive that names GCIH certification as proof that a DoD employee or contractor is capable of taking on the highest of three levels of technical cybersecurity roles in DoD. The GIAC certifications used for evaluating student mastery of course objectives are updated using a large-scale job-task analysis that interviews practitioners at least every three years. This process, along with the psychometric assessments that shaped question assessment, is subjected to regular review by the American National Standards Institute. GIAC exams increasingly include hands-on test questions where students can demonstrate they can use what they learned.

3. **To evaluate program outcomes,** STI tracks all graduates and asks them (and when possible, their employers) annually for feedback on how well the program worked for them and how it might be improved. Additionally, STI has implemented its formal Learning Outcomes Assessment Plan, as endorsed by the MSCHE evaluation team. Under this plan, each program undergoes a formal review by an evaluation team comprised of subject matter experts every four years. This review process will ensure alignment of (1) course outcomes to program learning objectives, of (2) program learning objectives to any capstone requirements, and of (3) both program learning objectives and capstone requirements to a survey of industry requirements. This request for substantial change is based upon the MSISE program review in 2019.

Consistency with the State’s Minority Student Achievement Goals

STI is committed to maintaining an environment of appropriate conduct among all persons and respect for individual values. The Institute is committed to enforcing non-discrimination and anti-harassment in order to create an environment free from discrimination, harassment, retaliation and/or sexual assault. Discrimination or harassment based on race, gender and/or gender identity or expression, color, creed, religion, age, national origin, ethnicity, disability, veteran or military status, sex, sexual orientation, pregnancy, genetic information, marital status, citizenship status, or on any other legally prohibited basis is unlawful and undermines the character and purpose of STI. Such discrimination or harassment will not be tolerated.

Relationship to Low Productivity Programs Identified by the Commission

This program is not related to an identified low productivity program.

Adequacy of Distance Education Programs

The combination of live classroom and three distance learning modalities used in the MSISE program was commended for its "creative and forward looking teaching methodology" in the April 2018 Team Report to the Middle States Commission on Higher Education. That report also noted that all modalities resulted in equivalent scores, with the distance learning modalities earning slightly higher scores in several tougher courses where students needed more time to absorb (and review) the material.

The three distance learning modalities available to students to complete the SANS technical course component are OnDemand, vLive, and Simulcast. Students who use the OnDemand platform are given access to a learning management system with modules pre-loaded into the system and are also provided with printed course books containing written lectures and labs. Each module is a recording from an in-person course session. The learning management system allows students to revisit lectures and also complete quizzes to verify understanding. A recommended viewing schedule is included in course syllabi. Each STI course has a responsible faculty member, who in most cases is the same person recorded for the OnDemand course system. A teaching assistant referred to as a virtual mentor is available for all OnDemand courses to help answer student questions or assist with lab issues.

The vLive learning modality is conducted online with established course meeting times led by an instructor – typically twice per week for up to eight weeks – through a learning management system that allows for direct interaction with the instructor and other course participants. Each course session is recorded for students to review previously covered material, or to view if they miss a session.

The Simulcast delivery modality allows students to participate in a course being offered through the in-person modality, but from their location of choice, enabled through a digital learning management system. Students meet during the same time the in-person course meets. They can participate in classroom lectures by seeing and hearing the instructor, in addition to asking questions and participating in classroom discussion.

If a student chooses a distance learning modality, that experience is comprised of the very same coherent, cohesive, and academically rigorous curriculum used for the course when taken via our traditional residential institute-based, in-person instructional format. The faculty member assigned to the STI course reviews student performance on exams and papers and assigns a grade at the end of the course.

1. **Curriculum and instruction**

   a) ***A distance education program shall be established and overseen by qualified faculty.***

   When implemented for distance education, the courses are converted from the live in- class courses in consultation with and under the direction of the faculty

   b) ***A program's curriculum shall be coherent, cohesive, and comparable in academic rigor to programs offered in traditional instructional formats.***

   If a student chooses a distance learning modality, that experience is comprised of the very same coherent, cohesive, and academically rigorous curriculum used for the course when taken via our traditional residential institute-based, in-person instructional format. The faculty member who oversees the STI course reviews student performance on exams and papers and assigns a grade at the end of the course. Moreover, the outcomes achieved by students employing STI's distance learning modalities are demonstrably equivalent to those achieved by students who attend live in-person courses.

   The working group for the 2014 Substantive Change Request, whereby STI was approved by Middle States to deliver more than 50 percent of our credit via distance modalities, reported:

> “A 2013 study of all certification exam results provided evidence that the exam scores achieved on these standardized certification exams were not statistically different when comparing delivery modalities – such as whether the course instruction was taken via our traditional, live instructional format or via either our OnDemand or vLive instructional modalities....A similar analysis was conducted using calendar year 2014 exam outcomes. Results from the analysis were consistent with trends noticed in the 2013 study of all certification exams. On average, students who enrolled in a distance education course in 2014 performed slightly better on exams than students who enrolled in in-person courses.”

To update these assessments, the working group once again compared the GIAC scores of students who had taken their classes live versus those who took their classes through STI’s OnDemand modalities, and once again found the measured learning outcomes to be the same among both groups (Table A4.1).

Table A2.1 Comparison of GIAC Exam Score Performance via Live and OnDemand Modalities, 2014-2017

Modality	Overall Score	Master’s Program	Certificate Program
Live Class	84.6	86.6	82.4
OnDemand Class	83.7	87.2	82.0

c) ***A program shall result in learning outcomes appropriate to the rigor and breadth of the program.***

The learning outcomes of the courses included in the Applied Cybersecurity Program have been validated by the faculty as appropriately rigorous and broad and are integrated into each course and measured quantitatively through ANSI-standardized certification exams for the three advanced courses and through integrated testing in each of the other courses.

d) ***A program shall provide for appropriate real-time or delayed interaction between faculty and students.***

A teaching assistant referred to as a virtual mentor is available for all OnDemand courses to help answer student questions or assist with lab issues.

The vLive learning modality is conducted online with established course meeting times led by an instructor – typically twice per week for up to eight weeks – through a learning management system that allows for direct interaction with the instructor and other course participants. Each course session is recorded for students to review previously covered material, or to view if they miss a session.

The Simulcast delivery modality allows students to participate in a course being offered through the in-person modality, but from their location of choice, enabled through a digital learning management system. Students meet during the same time that the in- person course meets. They can participate in classroom lectures by seeing and hearing the instructor, in addition to asking questions and participating in classroom discussion.

e) ***Faculty members in appropriate disciplines in collaboration with other institutional personnel shall participate in the design of courses offered through a distance education program.***

STI faculty members design all distance learning programs.

2. Role and mission

a) ***A distance education program shall be consistent with the institution’s mission.***

The distance education program at STI is identical in content and impact to the live training program and has been designed, with strong faculty leadership and deep embedded course and program assessment, to focus precisely on meeting STI's mission to develop leaders to strengthen enterprise and global information security.

b) ***Review and approval processes shall ensure the appropriateness of the technology being used to meet a program's objectives.***

The appropriateness of the technology STI uses for distance education has evolved over more than 11 years to be optimized for meeting the active learning needs of full-time working professionals, and it been assessed and approved by STI faculty. But that is not the end of the development process. The distance learning technology is continuously evaluated through evaluations completed by every one of the more than 3,000 cybersecurity professionals using it each day. If a course is not helping students master the key learning objectives, we hear about it quickly and fix the problems.

3. Faculty support

a) ***An institution shall provide for training for faculty who teach with the use of technology in a distance education format, including training in the learning management system and the pedagogy of distance education.***

Faculty who participate in our OnDemand, vLive, and Simulcast distance learning modalities undergo specific training to help modify their style to this format. We engage a team of individuals to assist in online-specific methods to enable virtual student-faculty interactions, including (when a class is Simulcast to students) employing an assistant in the room who participates in the class on behalf of distance students by flagging the instructor's attention when questions are asked or issues are raised by virtual students.

b) ***Principles of best practice for teaching in a distance education format shall be developed and maintained by the faculty****.*

Members of the STI faculty have developed guidelines for best practice when teaching in our distance education formats. The guidelines are reproduced below.

Instructor Guidelines for SANS Simulcast Classes

What to Expect
During a SANS Simulcast you will be teaching live students in the same room AND students at remote locations. To accomplish this, your on-site moderator will log into GoToTraining and our system will capture everything that is projected in the classroom. You will also wear a wireless microphone to transmit your voice to remote students. The moderator will also set up a webcam and broadcast video from the classroom. We highly encourage the use of video, but if you do not want video to run in your class, please contact the Simulcast staff.

All-day classes will be broken into two sessions: morning and afternoon. When you break for lunch please remind all students to log out of GoToTraining and to log into the afternoon session when they return. You will also need to do the same thing, so please return from your lunch break a few minutes early. The key to teaching a successful vLive! Simulcast is to always **remember that you are teaching remote students; keep them engaged** by promptly responding to their questions and periodically addressing them directly.

Advance Planning
1. The vLive! and Onsite teams will schedule a planning call with the customer point of contacts two weeks before the course; please plan on attending this call.

2. The AV kit that contains all necessary equipment for the Simulcast will be shipped to the Simulcast location prior to class.
3. The vLive! support team will be setting up the audio equipment and test the setup with you. This test is critical to the success of the Simulcast session and must be completed prior to starting class.
4. If it is possible, plan to do the audio testing the day before class starts. If this is not possible please make sure you arrive 2 hours early on the first day of class to complete the audio setup.
5. The vLive! team will introduce you to the virtual moderator who will be working the classroom. This moderator is a SANS employee who is there to assist with the running of the Elluminate platform, running labs, and assisting with student questions. Many instructors prefer that the moderator relays questions from the virtual students by raising his or her hand and reading the question.

Audio Tips

6. Do not wear your cell phone on your belt next to the transmitter or lay it next to the receiver by the laptop. Your cell phone and student cell phones can create interference. You may need to disable Bluetooth functionality on your phone if it is causing buzzing.

7. Leave your wireless microphone on at all times, but turn off your GoToTraining audio during breaks. To do this, simply ask your on-site moderator to mute you on the Simulcast laptop.

8. ALWAYS repeat comments and questions from students at your location; remote students can hear you, but all other sound will be muffled or inaudible.

Starting Class

9. When it is time to start class, your moderator will start the recording and give you a signal that everything is ready on the remote side.

10. After the moderator has turned the class over to you, introduce yourself and briefly explain to students how the Simulcast class will work.

11. It is important to make the remote and on-site students aware of each other. Identify and welcome each remote site by name. A roster with the remote sites and student counts will be provided to you.

12. Please encourage remote students to participate by typing their questions and comments into the Chat window.

13. Directing questions about class material to the virtual students can also help to keep them engaged throughout the class.

14. The moderator will relay any questions from the online students to you.

15. Discuss any other housekeeping items as needed (timing of breaks, confirming that VMWare is correctly set up, etc.).

Teaching Tips

16.ALWAYS repeat comments and questions from students at your location; remote students can hear you, but all other sound will be muffled or inaudible.

17. If you need to discuss issues that students should not see, please use the “Organizers Only” or “private message” chat option as your means of communication.

18. Address remote students often to ensure they feel like they are part of the class; remote students become passive listeners if they are not actively engaged.

19. All scripts, videos, demos, etc. that you wish to show to students must be shared with GoToTraining’s application sharing feature.

20. Remote students’ systems (and your host’s network) can be slowed down if you send very large files. If a file is necessary for class try to send it before class or during a break. If it is not course-related (e.g., music while on break), consider not sending it.

21. Use the GoToTraining timer when breaking from lecture so remote students know when class will be resuming; tell the moderator how many minutes you would like and they will set up the timer for you.
22.When breaking for lunch, please explain to students that they will need to log out of the morning session and log into the afternoon session upon their return.

23. Allow plenty of time to log into GoToTraining when arriving in the morning or returning from lunch. Depending on the location, you may have to extend the lunch break.

24. Conduct a quick audio check after each break and lunch to confirm that your microphone is on and that your remote students can hear you.

Suggested Best Practices
Jason Fossen:

- Each day I used a second laptop to log onto vLive as an attendee so that I could see how fast my application sharing window was updating its screen. It was also useful for checking the sound, video, and file-sharing features. I granted my other account moderator status so that, in case my primary laptop had an issue, I could switch over to the secondary and continue teaching.
- New vLive instructors (or new laptops for prior instructors) should go through the setup and test process before flying on-site; there won't be enough time to fix any problems like these the morning of.
- Return early after lunch to log back into GoToTraining
- Make sure your Internet connection is wired and not shared by the students.
- Make sure to have the vLive emergency contact info on hand.
- The instructor should have the slides to teach the course on his/her laptop in case the slides in the vLive system are missing, wrong, or have any problems.

Jason Lam:

- Make sure that the OnSite students are aware of the virtual students.
- Be available for remote students before or after class in the Elluminate Office session.
- Depending on the class size and your teaching style you might need longer than usual to prepare for class (questions, demos, labs).
- Have the moderator type names of products, vendors, URLs, etc. in the chat for the virtual students.

c) ***An institution shall provide faculty support services specifically related to teaching through a distance education format.***

SANS Simulcasts are supported by the Onsite and vLive teams. The Onsite team takes the lead with most sales issues, while the vLive team provides most of the support during class. While you are teaching you will have one or more vLive moderators in the vLive virtual classroom to provide assistance with labs and logistics.

4. An institution shall ensure that appropriate learning resources are available to students including appropriate and adequate library services and resources.

The challenges of information security are constantly evolving, and excellence in performance demands continuous monitoring of changes in threats, technology, and practices. SANS conducts an extensive research program that helps STI students and alumni maintain their edge in security. The SANS Resource Center is a compilation of thousands of original research papers, security policies, and security notes, along with a wealth of unique network security data. The list below outlines some of the primary resources available.

- The SANS Information Security Reading Room contains more than 2,000 original research studies, not available from any other source, in 76 knowledge domains relevant to the study of information security. They are downloaded more than a million times each year. The Reading Room is available at http://www.sans.org/reading_room/.
- The SANS Security Policy Collection contains model security policies developed by major corporations and government agencies. The collection contains about 35 policies and grows as new security issues arise and policy templates are needed.
- The SANS Top-20 V7 is a consensus list of vulnerabilities that require immediate remediation. It is the result of a process that brought together dozens of leading security experts.
- The SANS Newsletter Collection helps keep students up to date with the high-level perspective of the latest security news.
- The Security Glossary is among the largest glossaries of security terms available on the Internet. It was developed jointly by SANS and the National Security Agency and provides authoritative definitions of many of the specialized terms students will encounter.
- The SANS Collection of Frequently Asked Questions about Intrusion Detection contains 118 authoritative discussions of the primary topics that arise when planning and implementing intrusion detection technologies. The collection is available at http://www.sans.org/security-resources/idfaq/.
- The SANS Internet Storm Center Archives contain contemporaneous analyses of new attacks that are discovered on the Internet. The archives constitute an extraordinary research asset because of the depth of the analysis and the currency of the topics covered. They also provide SANS students with access to raw data, summaries, and query facilities to analyze malicious Internet traffic records. This is a rich data source for advanced security research projects that analyze attack patterns and how fast worms spread through the Internet.
- SANS Web Briefings held several times a month feature SANS faculty and other security experts providing up-to-date web briefings for SANS alumni on new threats seen at the Internet Storm Center, new technologies that are emerging, and analysis of security trends.

5. Students and Student Services

a) A distance education program shall provide students with clear, complete, and timely information on the curriculum, course and degree requirements, nature of faculty/student interaction, assumptions about technology competence and skills, technical equipment requirements, learning management system, availability of academic support services and financial aid resources, and costs and payment policies.

- Curriculum information is posted, in detail, at the SANS.EDU website at https://www.sans.edu/academics/
- Course and degree requirements are posted online in the STI Course Catalog at https://www.sans.edu/downloads/STI-Course-Catalog-2018.pdf
- The nature of faculty/student interaction are described on our website at https://www.sans.edu/academics/course-delivery/more
- Assumptions about technology competence and skills are posted at our Admissions website at https://www.sans.edu/admissions/masters-programs
- Technical equipment requirements are posted with individual courses at the SANS course website.
- Learning management systems information is posted in detail at https://www.sans.org/ondemand/faq
- The availability of academic support services and financial aid resources is posted at https://www.sans.edu/students/services, and on page 33 of the Student Handbook at page 33, https://www.sans.edu/downloads/sti-student-handbook.pdf

- Costs and payment policies are posted at https://www.sans.edu/admissions/tuition

b) ***Enrolled students shall have reasonable and adequate access to the range of student services to support their distance education activities.***

With STI students taking approximately half of their credits through distance learning, the overall satisfaction with student services may be considered a reliable surrogate for effectiveness of distance learning student services. Evidence from student surveys indicates that measures of overall student satisfaction are high (above 90%).

Quantified measures of specific sub-processes with student management were also high, with about 90% of respondents saying they were "Somewhat Satisfied" and "Very Satisfied" for each of the operational elements (Table A.4.2).

Table A.2.2. Student Satisfaction with Student Management as Reported in the 2016 Student Experience Survey

	Very Dissatisfied	Somewhat Dissatisfied	Somewhat Satisfied	Very Satisfied
Registration/Billing	<1%	10%	21%	68%
Academic Advising	2%	8%	25%	65%
GI Bill Certification	2%	6%	17%	75%

c) Accepted students shall have the background, knowledge, and technical skills needed to undertake a distance education program.

Our MSISE students are working professionals with at least one year of experience in information technology or information security. Thus, they have the needed background, knowledge, and technical skills to use the distance learning modalities.

a) ***Advertising, recruiting, and admissions materials shall clearly and accurately represent the program, and the services available***

STI has a solid record of meeting Middle States' high standards for transparency and accuracy in all its marketing and admissions materials and will continue to do so. Advertising, recruiting, and admissions materials for MSISE students were available in the Resource Room during our 2017 MSCHE and MHEC evaluation team visit.

5. Commitment to support

Every teacher is evaluated every day by every student, and those evaluations specifically measure the teachers' effectiveness in distance education. Those evaluations affect teachers' compensation as well as their long-term career prospects with STI.

a) ***Policies for faculty evaluation shall include appropriate consideration of teaching and scholarly activities related to distance education programs.***

Every teacher is evaluated every day by every student, and those evaluations specifically measure the teachers' effectiveness in distance education. Those evaluations affect teachers' compensation as well as their long-term career prospects with STI.

b) ***An institution shall demonstrate a commitment to ongoing support, both financial and technical, and to continuation of a program for a period sufficient to enable students to complete a degree or certificate.***

STI has adequate faculty, infrastructure, and financial resources, as demonstrated in Sections H, J, and K, to maintain the MSISE program.

6. Evaluation and assessment

a) ***An institution shall evaluate a distance education program's educational effectiveness, including assessments of student learning outcomes, student retention, student and faculty satisfaction, and cost-effectiveness.***

STI employs a three-level evaluation program completely embedded in the curriculum. The 2018 Middle States Evaluation Team commended this evaluation methodology: "SANS Technology Institute should be commended for the fact that its curriculum automatically embraces learning outcomes and program outcomes." The assessment system and processes are detailed in the evaluation section of this document. This same system will be used in the distance learning component of the MSISE program.

b) ***An institution shall demonstrate an evidence-based approach to best online teaching practices.***

STI online teaching practices are currently in use by more than 3,000 students, and at least 50,000 students have used it during the past eight years. Each of those students evaluates the effectiveness of the learning modality in every course, and we continually improve the practices to ensure those ratings continue to match or exceed live classroom training scores.

c) ***An institution shall provide for assessment and documentation of student achievement of learning outcomes in a distance education program.***

Ultimate student achievement in the MSISE program will be measured by grades on the internationally standardized GIAC exams for each area of security. We compare these scores in distance and in-person learning modalities. As shown in Table A.4.3, the GIAC test scores in distance learning are essentially identical to scores of students who used live, in-person residential training programs:

Table A.2.3. Comparison of GIAC Exam Score Performance via Live and OnDemand Modalities, 2014–2017

Modality	Overall Score	Master's Program	Certificate Program
Live Class	84.6	86.6	82.4
OnDemand Class	83.7	87.2	82.0

We will continue to monitor GIAC scores in the MSISE program, by delivery modality.

Appendix 1. Contracts with Related Entities

The SANS Technology Institute (STI) as an educational institution is an independent yet symbiotic and related entity to the much larger SANS and GIAC organizations. As such, it represents a unique integration of existing and purpose-built educational elements from SANS and GIAC, augmented with additional elements that are specific to STI:

- **STI as an independent subsidiary** – STI is an independent but wholly owned subsidiary of SANS, with its own board and administrative staff. As an organization, it is designed to include those full-time personnel who directly serve the admissions and ongoing management and educational servicing of students, while outsourcing most other functions to SANS and GIAC, which operate at scale and may deliver those services (including human resources, finance, and technology systems) to STI at levels or costs that would otherwise be unachievable by an institution with fewer than 1,000 students. This unique combination of dedicated staff and flexible access to world-class scale and quality systems is a key enabler for STI's students to access world-class faculty and educational content from an otherwise small institution.

- **STI's faculty come from SANS** - STI's faculty is comprised of and appointed from the 85 individuals who have achieved the status of being "SANS Certified Instructors," an industry-recognized demarcation of technical achievement practiced in the field, superior teaching effectiveness, capacity to engage students as exemplified in the classroom and online, and successful completion of a competitive development process that employs both student and peer-faculty feedback to prove that the instructors possess these qualities. Among the faculty are people who are called upon to investigate attacks on the U.S. government and the country's largest commercial enterprises, who are entrusted to teach practitioners of cybersecurity at the highest and most sensitive (classified) levels, and who through their professional practice and research advance our understanding of cyber threats and potential remediation, and then transmit that knowledge forward to our students and the larger community. Even beyond their superlative technical abilities, our faculty members have skills as teachers that truly set them apart and allow them to impart sometimes dense technical lessons with enthusiasm, applicable real-world examples, and charismatic engagement. While a handful of faculty members serve in full-time teaching and research roles, most are scholar-practitioners who teach less than full-time for the school so that they can engage in the practice of cybersecurity, keep their skills advanced and current, and feed their experiences and learning back into the courses and class discussions.
- **STI's programs designed by STI faculty** – STI's academic programs were designed by the faculty in order to optimally achieve their stated learning outcomes. For each program, the faculty responsible for program design built out the educational content from three distinct sources:

    - **SANS Technical and Management Courses** – SANS maintains the world's largest and most-respected catalog of 36-50 seat-hour courses in cybersecurity, ranging from broad survey courses in cyber defense to highly advanced and specialized penetration testing and digital forensics courses. Each program includes a subset of SANS courses relevant to achieving that program's learning outcomes, including the availability of elective courses. In addition, STI students may avail themselves of all the opportunities at different times and locations throughout the United States (and world) that the courses are offered live and taught by STI faculty, or they may also take the opportunity to take the very same course presented online by SANS, which transforms the best live performance by an STI faculty member into the online version of the course, complete with the same labs and access to subject-matter experts online. STI thereby offers an extraordinarily broad set of choices for students to tailor their program schedule to fit within their work and personal lives.

    - **GIAC Certification Exams** – STI's faculty deploy various world-class, industry- proven GIAC examinations to validate the learning achieved by each student in a SANS technical course. GIAC exams result from an exam development effort that far exceeds the typical requirements for college-level examinations. That effort includes job task analyses to ensure relevance and psychometric reviews that in turn ensure appropriate difficulty and rigor. Many of the GIAC exams deployed in STI's programs are themselves ANSI-certified for quality and robustness. The use of those exams enables STI's programs to ensure that students are assessed fairly and that their performance and grades are constantly level-set against the performance of other industry professionals taking the same exam.

- **STI-specific educational elements and courses** – STI's faculty creates many additional elements to augment the programs with written security memos and research, oral presentations, group projects, and other experiences designed to require high-level integrations of learning.

This Memoranda of Understanding (MOU) defines the business relationships between STI, its SANS parent, and its sister organization the Global Information Assurance Certification (GIAC) organization.

Memorandum of Understanding
between
The SANS Technology Institute ("STI")
and
The Escal Institute of Advanced Technologies ("SANS")

Agreement Published Date: January 1st, 2018
Agreement Period of Performance: January 1st, 2018 – December 31st, 2025

Purpose

The purpose of this Memorandum of Understanding ("MOU") is to establish a cooperative partnership between the SANS Technology Institute (STI) and the ESCAL Institute of Advanced Technologies, Inc/dba/SANS Institute (SANS). This MOU will:

- outline services to be offered by SANS to STI;
- quantify and measure service level expectations, where appropriate;
- outline the potential methods used to measure the quality of service provided;
- define mutual requirements and expectations for critical processes and overall performance;
- strengthen communication between the provider of administrative services (SANS) and its enterprise customer (STI);
- provide a vehicle for resolving conflicts.

Vision

SANS will provide a shared business environment for the STI enterprise. The business environment will continuously enhance service, compliance and productivity to STI's employees, students and core administrative practices. The primary goals for the MOU include:

- **Integrate** people, processes, and technology to provide a balanced service level to all customers. Create a collaborative environment where trusted relationships and teamwork are encouraged between administrative services, departmental staff, faculty, students and suppliers to further the enterprise's goals.
- **Leverage** human resources, institutional knowledge, developing skill sets, and technology in an effort to continuously improve service and productivity for all services provided. Create an organizational structure that balances STI's strategic and tactical efforts to promote efficiencies.
- **Mitigate** risk to the STI enterprise by focusing on compliance requirements and understanding the impact these requirements have on productivity and student services. Develop an integrated organizational structure that will promote the consistent interpretation and enforcement of policies, procedures, local, state and Federal laws and regulations throughout the enterprise.

Mission

Through various SANS educational and administrative service units, provide business activities dedicated to operational and student service excellence to the STI enterprise so that core STI staff can focus on the academic components of their mission to educate managers of information security groups and technical leaders who direct information security programs.

Scope

The SANS Institute will provide access for STI students, in all delivery modalities, to the Technical courses offered by the SANS Institute that are a part of STI's course curricula, including, Course Maintenance, Presentation of this course material , and Educational Residency services for the SANS Technology Institute. The SANS Institute shall provide policy-compliant management of Accounting & Finance, Bursar & Registration, Human Resource, Marketing, and Information Technology infrastructures for STI.

Hours of Operations

Typical staffed hours of operation for the SANS activities are 9:00 – 5:00 Monday-Friday, with the exception of approved holidays. Working hours may be adjusted due to system/power outages, emergency situations, or disaster. Through the use of technology, it is expected that many of the services provided will be available to STI students and employees on a 24-hour basis.

Service Expectations

SANS and STI agree to the service expectations and working assumptions listed below. These service expectations are meant to monitor the more critical elements of the services provided and are not meant to reflect the comprehensive services offered by SANS. The productivity indicators reflected below are not listed in any order of priority.

Accounting and Finance

Process	**Service Expectation**	**Service Metric**
Accounts Receivable	Remittances produced in the form of check, EFT, or wire.	Payment schedule is set up for a daily cycle and reporting available daily.
Payment accuracy	All payments made will be for approved and legitimate services/products	Audits of vendor transactions will show evidence of 100% three-way match.
Employee travel and expenses are reimbursed.	Protect financial outlays made by employees.	Reimbursements are made within a 30-day timeframe.
Financial reporting	Financial reporting is done on time and in accordance with the same audited accounting principles used by SANS.	All MSCHE, federal and internal reporting deadlines will be met on time.
Audit of records	Annual audits will be performed	Annual audit performed on the Financial Statements by an independent external auditor

Bursar & Registration

Process	**Service Expectation**	**Service Metric**
Cashier Function	Process payments and distribute revenue to appropriate departments	Payments will be processed within 24 hours of receipt, and revenue distributed on a monthly basis

Human Resources

Process	**Service Expectation**	**Service Metric**
Benefits	Provide benefits which are in the best interest of the employees and employer	Annual survey of employees will show that major benefits of interest are being adequately provided

Payroll	Assure timely payroll and employee reviews	All bimonthly payrolls will be made on the 15th and final days of the month
HR services	Manage HR service to ensure receipt by employees	HR services are provided for in a timely manner as measure in annual survey and changes are communicated and enforced

Marketing

Process	Service Expectation	Service Metric
Brand Awareness	Create awareness of STI programs within the information Security Community	SANS will facilitate access to its customer list and will routinely conduct cross-branding to assist with market awareness of STI graduate programs
Technical Expertise	SANS will provide the creative content assistance, graphic editing, and industry expertise required to allow for the execution of STI recruitment campaigns	Generalized STI marketing campaigns are made operational via the availability of a centralized SANS marketing staff

Information Technology

Process	Service Expectation	Service Metric
Digital learning environment	Create and maintain a leading edge digital environment for learners	Learner surveys consistently scoring above 4 on a scale from 1 to 5, plus recommender percentage greater than 90%.
Technology infrastructure	Provide transaction platforms to support student course registration and other services	Annual surveys of students to reflect adequacy of transaction processes

Technical Course Maintenance & Presentation

Process	Service Expectation	Service Metric
Currency of content	Make available for use by STI Faculty any and all technical content developed by the SANS Institute	Content is reviewed at least semi-annually for currency with existing malicious capabilities and mitigation theory and strategy
Quality of content and presentations	Assist through all means necessary and available the delivery of STI	SANS Institute will make available all performance ratings derived

	faculty and lab instruction in a high-quality fashion	from students on STI courses or faculty

Educational Residency

Process	Service Expectation	Service Metric
Conference services	Provide hotel, classroom technology, refreshment and other services that promote an unencumbered learning environment for students	Conference services provided will maintain an average rating of at least 4 out of 5 on daily student surveys

Service Constraints

- ***Workload -*** Increases in workload, such as back log due to power outages or fiscal year end closing, may result in temporary reduction of service level delivery.
- ***Conformance Requirements -*** Finance policy changes and Internal Revenue regulations may alter procedures and service delivery timeframes.
- ***Dependencies -*** Achievement of the service level commitment is dependent upon student and employee compliance with the policies and procedures of the STI enterprise.

Terms of Agreement

The term of this agreement is January 1, 2018 - December 31, 2025. This Agreement may be cancelled only by STI, at its sole discretion.

Periodic Quality Reviews

STI and SANS will jointly conduct periodic reviews of individual SANS administrative support unit performance against agreed-upon service level expectations. The agenda for these reviews should include, but is not limited to:

- service delivery since the last review
- major deviations from service levels
- conflicts or concerns about service delivery
- planned changes to improve service effectiveness
- provide feedback from student and employees
- annual customer satisfaction surveys

STI and SANS will also regularly assess customer satisfaction and will use the results as a basis for changes to this Agreement.

STI's Executive Director and the SANS administrative service unit lead will meet annually.

Service Level Maintenance

This Agreement will be reviewed on an ongoing basis and updated as needed. Revisions may become necessary due to changing service needs, modifications to existing services, addition of services, significant variations from agreed upon-service levels, or unanticipated events.

Issue Resolution

- If either party identifies a substantive breach of responsibility, or other problem that requires resolution prior to the next periodic review, the operating level managers of both parties will engage in a joint effort of understanding and rectification of the issue. In the event this remedial effort fails, either party can raise the issue to the executive levels of both parties.

Payment Terms and Conditions

For services provided, STI will pay SANS according to the following schedule:

- STI will pay SANS $1,500 for each instance when an STI student registers for a full SANS class as part of an STI course, regardless of the chosen delivery modality (live event or online), and as subject to the schedule found at Appendix A for partial or non-standard classes which comprise only 1-credit events within the STI curriculum.
- STI will pay amounts to SANS, monthly in arrears, to reflect any directly allocated expenses by SANS personnel in support of STI business according to this services agreement (specifically including the result of any time allocation procedures as determined by SANS accounting department)
- STI will pay an amount to SANS, monthly in arrears, to reflect its pro-rata share of SANS' otherwise unallocated costs for Accounting & Finance, Bursar, Human Resource, Marketing and Information Technology, and related administrative services, in proportion to its share of revenue relative to SANS revenue also sharing in this services pool.

Agreed to on behalf of STI: Agreed to on behalf of SANS:

__________________________ ____________________________

Eric A. Patterson
Executive Director
SANS Technology Institute

Peggy Logue
Chief Financial Officer
SANS Institute

__________________________ ____________________________

Date: Date:

Appendix A: Schedule of SANS Courses Subject to, or Exempt From, the Payment Terms Described in this Agreement

STI Course	SANS Course	Payment Amount
ISE 5101	SEC 401	$1,500
ISM 5101	MGT 512	$1,500
ISE/M 5201	SEC 504	$1,500
ISE/M 5300	MGT 433	$ 500
ISM 5400	MGT 514	$1,500
ISE 5401	SEC 503	$1,500
ISE/M 5500	N/A	$ 0
ISE 5600	MGT 514 (Day 4)	$ 500
ISM 5601	LEG 523	$,1500
ISE/M 5700	N/A	$ 0
ISE/M 5800	MGT 525	$1,500
ISE/M 5900	N/A	$ 0
ISE/M 6001	SEC 566	$1,500
ISE/M 6100	N/A	$ 0

ISM 6201	AUD 507	$1,500
ISE/M 6215	SEC 501	$1,500
ISE 6230	SEC 505	$1,500
ISE 6235	SEC 506	$1,500
ISE 6240	SEC 511	$1,500
ISE/M 6300	NetWars	$ 0
ISE 6315	SEC 542	$1,500
ISE 6320	SEC 560	$1,500
ISE 6325	SEC 575	$1,500
ISE 6330	SEC 617	$1,500
ISE 6350	SEC 573	$1,500
ISE 6360	SEC 660	$1,500
ISE 6400	DFIR NetWars	$ 0
ISE 6420	FOR 500	$1,500
ISE 6425	FOR 508	$1,500
ISE 6440	FOR 572	$1,500
ISE 6450	FOR 585	$1,500
ISE 6460	FOR 610	$1,500
ISE 6515	ICS 410	$1,500
ISE 6520	ICS 515	$1,500
ISE 6615	DEV 522	$1,500
ISE 6715	AUD 507	$1,500
ISE 6720	LEG 523	$1,500
RES 5500	N/A	$ 0
RES 5900	N/A	$ 0