SANS Technology Institute

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

ALAN PALLER
President

DAVID HOELZER
Dean of Faculty

JOHANNES ULLRICH, Ph.D.
Dean of Research

TIM MEDIN
MSISE Program Director

ERIC PATTERSON
Executive Director

SHELLEY MOORE
Assistant Director

BETSY MARCHANT
Assistant Director,
School Operations

August 01, 2018

James D. Fielder, Jr., Ph.D.
Secretary of Higher Education
Maryland Higher Education Commission
Nancy S. Grasmick Building, 10th floor
6 North Liberty St.
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

PROPOSAL FOR A SUBSTANTIAL MODIFICATION TO THE EXISTING DEGREE PROGRAM: MASTER'S OF SCIENCE IN INFORMATION SECURITY ENGINEERING

SANS Technology Institute

MARYLAND HIGHER EDUCATION COMMMISSION

ACADEMIC PROGRAM PROPOSAL

PROPOSAL FOR:

______NEW INSTRUCTIONAL PROGRAM

__x__ SUBSTANTIAL EXPANSION/MAJOR MODIFICATION

_____ COOPERATIVE DEGREE PROGRAM

__x___WITHIN EXISTING RESOURCES or_____REQUIRING NEW RESOURCES

The SANS Technology Institute
Institution Submitting Proposal

September 1, 2018
Projected Implementation Date

Master's of Science
Award to be Offered

Information Security Engineering
Title of Proposed Program

5199
Suggested HEGIS Code

11.1003
Suggested CIP Code

SANS Technology Institute
Department of Proposed Program

Tim Medin
Name of Department Head

Tim Medin
Contact Name

tmedin@sans.edu
Contact E-mail Address

(612) 205-1840
Contact Phone Number

President/Chief Executive Approval

____
Signature and Date

N/A – incremental changes over time
Date Endorsed/Approved by Governing Board

Table of Contents

SANS Technology Institute

Program Proposal for a Substantial Modification

Master of Science in Information Security Engineering

August, 2018

A. Program Summary and Centrality to Institutional Mission Statement and Priorities

1. Program Description

This proposal of substantial modification is the result of minor program modifications which have occurred over time since 2014, which have been collectively assessed by STI, MHEC, and MSCHE during our recent self-study and reaffirmation of accreditation, and which have, in the estimation of both STI and MHEC, reached the cumulative threshold of substantive change.

The program leading to a Master of Science in Information Security Engineering (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. While the program cannot be completed entirely at-a-distance, most of the courses are offered in multiple formats, allowing an individual student the option to take more than 50% of the program at-a-distance using one or more of our online modalities, or, conversely, to take 50% or more of the 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 formal 'focus areas' available, whereby students may make elective choices that coincide with the areas of Blue Team Operations, Penetration Testing, Digital Forensics and Incident Response, Enterprise Security Management, and Industrial Control Systems.

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

> The SANS Technology Institute develops technically-skilled leaders to strengthen enterprise and global information security. STI enables full-time working professionals to learn advanced practices and management techniques from faculty who are top scholar-practitioners in the industry, and to integrate real-world applied research into their graduate education.

The formal Vision of the SANS Technology Institute is:

> The SANS Technology Institute aspires to be the preeminent graduate institution translating contemporary information security practice and scholarship into effective educational experiences. Our graduates will be highly valued because they design state-of-the-art, enterprise-level cyber defenses, champion the adoption of those defenses, and manage their implementation and ongoing operation.

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 therefore fits directly within the focused mission of the SANS Technology Institute in developing both managers of information security groups and technical experts who lead information security technology programs.

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 focus areas 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.

Summary of key elements of incremental substantial modification

Program Learning Outcomes

At the time of our previous substantive change to the MSISE program in 2014, we listed eight program learning outcomes:

- 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.

Since 2014, we have added two additional program learning outcomes:

- 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.

Graduation Requirements

To a large degree, and as will be discussed below in the comparative course descriptions, little of real substance has changed with regards to the concepts, content, or course level learning outcomes associated with any given course, practicum, or project. However, we have substantially revised course numbers or modified course names as content has been updated, reflective of new iterations of original courses. We have also separated some requirements that were formerly bundled and packaged together requirements that were formerly separate. Thus we have also, where appropriate, re-balanced the credit hours within the program while maintaining an overall and unchanged credit load of 36 hours.

In 2014, students in the MSISE program were required to complete 36 credit hours via the following requirements:

2014 Graduation Requirements

Required Course	Credits
ISE 5000 Research & Communications Methods	0.5
ISE 5100 Enterprise Information Security	4
ISE 5200 Hacking Techniques & Incident Response	4
ISE 5300 Building Security Awareness	1
ISE 5400 Advanced Network Intrusion Detection & Analysis	4
ISE 5500 Research Presentation 1	1
ISE 5600 IT Security Leadership Competencies	1
ISE 5700 Situational Response Practicum	1
ISE 5800 IT Security Project Management	3
ISE 5900 Research Presentation 2	1
ISE 6000 Standards Based Implementation of Security	4
ISE 6100 Security Project Practicum	2
ISE 6900 Information Security Fieldwork	0.5
Technical Electives (3 courses)	9
Required Program Capstone - GIAC Security Expert exam	0
Total	36

Currently, MSISE students complete 36 credit hours via the following requirements. Comparative notes reflecting key changes from the 2014 graduation requirements in are included in this table:

2018 Graduation Requirements

Required Course	Course Name	Credits	Notes
ISE 5101	Security Essentials	3	Formerly ISE 5100, now minus research paper currently in ISE 5501
ISE 5201	Hacking Techniques & Incident Response	3	Formerly ISE 5200, now minus new ISE 6300 NetWars Practicum
ISE 5300	Building Security Awareness	1	No change
ISE 5401	Advanced Network Intrusion Detection & Analysis	3	Formerly ISE 5400, now minus research paper currently in ISE 5901
ISE 5501	Technical Research & Communication Practicum	3	Combined prior research paper (from former ISE 5100) & presentation (from former ISE 5500) requirements into a new course
ISE 5600	IT Security Leadership Competencies	1	No change
ISE 5700	Situational Response Practicum	1	No change
ISE 5800	IT Security Project Management	3	No change
ISE 5901	Advanced Technical Research & Communication Practicum	3	Combined prior research paper (from former ISE 5400) & presentation (from former ISE 5900) requirements into a new course
ISE 6001	Standards Based Implementation of Security	3	Formerly ISE 6000, revised credit count, eliminated third paper requirement from the program
ISE 6100	Security Project Practicum	1	Revised credit count
ISE 6300	NetWars Continuous Practicum	1	NetWars practicum separated from former ISE 6300
ISE 6999	Elective Courses	9	No change
ISE 7000	GIAC Security Expert Certification Technical Capstone	1	1 credit hour re-allocated to reflect preparation time and test time for capstone
Total		36	

To contextualize the nature of the curriculum changes we have listed key changes below, with commentary.

Curriculum v3.0 – April, 2014	Curriculum v3.3 – August, 2018
Name: “ISE 5000 Research & Communications Methods” Course elements: - Course content, MGT 305 - Creation of an annotated bibliography - Editing test - Oral presentation 0.5 credit hour	Removed from curriculum
Summary of changes: This course was removed from the curriculum, with similarly supporting course content and assignments embedded into ISE 5501 and ISE 5901.	

Curriculum v3.0 – April, 2014	Curriculum v3.3 – August, 2018
Name: “ISE 5500 Research Presentation 1” Course elements: - Creation and delivery of presentation derived from research paper 1 credit hour	Removed from curriculum
Summary of changes: This course was removed from the curriculum, with the presentation now embedded into ISE 5501.	

Curriculum v3.0 – April, 2014	Curriculum v3.3 – August, 2018
Name: “ISE 5900 Research Presentation 1” Course elements: - Creation and delivery of presentation derived from research paper 1 credit hour	Removed from curriculum
Summary of changes: This course was removed from the curriculum, with the presentation now embedded into ISE 5901.	

Curriculum v3.0 – April, 2014	Curriculum v3.3 – August, 2018
Name: “ISE 5100 Enterprise Information Security” Course elements: - Course content, SEC 401 - GSEC exam - Research Paper 4 credit hours	Name: “ISE 5101 Security Essentials” Course elements: - Course content, SEC 401 - GSEC exam 3 credit hours
Summary of changes: Removed the embedded research paper requirement to become its own, separate course (ISE 5501).	

Curriculum v3.0 – April, 2014	Curriculum v3.3 – August, 2018
Name: “ISE 5200: Hacking Techniques & Incident Response” Course elements: - SEC 504 class instruction - GCIH exam - NetWars simulation experience 4 credit hours	Name: “ISE 5201: Hacking Techniques & Incident Response” Course elements: - SEC 504 class instruction - GCIH exam 3 credit hours
Summary of changes: Removed the NetWars Continuous requirement to become its own, separate course (ISE 6300).	

Curriculum v3.0 – April, 2014	Curriculum v3.3 – August, 2018
Name: “ISE 5400 Advanced Network Intrusion Detection & Analysis” Course elements: - Course content, SEC 503 - GCIA exam - Research Paper 4 credit hours	Name: “ISE 5401 Advanced Network Intrusion Detection & Analysis” Course elements: - Course content, SEC 503 - GCIA exam 3 credit hours
Summary of changes: Removed the embedded research paper requirement to become its own, separate course (ISE 5901).	

Curriculum v3.0 – April, 2014	Curriculum v3.3 – August, 2018
Name: “ISE 6000 Standards Based Implementation of Security” Course elements: - Course content, SEC 566 - GCCC exam - Research Paper 4 credit hours	Name: “ISE 6001 Advanced Network Intrusion Detection & Analysis” Course elements: - Course content, SEC 566 - GCCC exam 3 credit hours
Summary of changes: Removed the requirement for a third research paper within the program.	

Curriculum v3.0 – April, 2014	Curriculum v3.3 – August, 2018
Name: Required Program Capstone - GIAC Security Expert exam 0 credit hours	Name: ISE 7000, GIAC Security Expert Certification Technical Capstone 1 credit hour
Summary of changes: Allocated one credit hour for the lengthy and substantial amount of preparation, practice exercises, skills seminars, one-day practice exam, and two-day formal exam.	

All other changes described in the tables above reflect the marginal re-allocation of credit hours based upon an increasing number of student experiences with these requirements, upon which we are able to refine assessments of the amount of work performed for a given requirement.

An analysis of all changes, for each course, indicate that approximately 90% of the student work required remains unchanged since 2014, though 60% of the courses have been renamed and/or reorganized as separate courses (e.g., research papers) for purposes of the new version 3.3 curriculum, with a corresponding re-allocation of credit hours across this revised curriculum.

2. Relation to STI Mission and Strategic Goals

The SANS Technology Institute is tightly 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:

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

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

Goal 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. Changes in how the MSISE program is managed have increased transparency in presenting course requirements and have provided faculty the freedom to use different pedagogical techniques to ensure that students meet established learning outcomes with increased support and focus.

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

1. Critical Need

Technological progress is a primary demonstration of, and the direct result of, the advancement and evolution of knowledge. Together with the increased prevalence in the use and applicability of information technology, and the benefits of substantial increases in productivity and efficiency this provides, comes the need to protect information-based assets from new adversaries, criminals, foreign nation-states, and vectors of attack. 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.

2. Alignment with the 2017–2021 Maryland State Plan for Postsecondary Education

New partnerships between colleges and businesses

The STI MSISE program supports the 2017 - 2021 Maryland State Plan for Postsecondary Education via Strategy 8, which states: “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 33,000 information security workers employed in Maryland, the state currently has more than 15,000 job openings in the field, with more than 3,000 of those positions categorized as being in the “Oversee and Govern” domain according to the NICE Cybersecurity Workforce Framework.

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

The National Institute of Standards and Technology (NIST) supports a website of data on cybersecurity jobs called CyberSeek that lists the number of current job openings by state and metropolitan area. In this section we combine the 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.

CyberSeek states that the supply of cybersecurity workers nationally is “very low,” with 285,681 job openings relative to a total employed workforce of 746,858 (a ratio of 0.38, or, “for every 100 employed workers, the market seeks another 38 people”). The ratio of “openings requesting a GIAC certification” to “holders of GIAC certifications” is nearly twice as low at 0.64 (or, “for every 100 current GIAC certification holders, the market seeks another 64”). CyberSeek estimates the number of current cybersecurity job openings in Maryland at 15,165, which is not inconsistent with the DLLR numbers. And, CyberSeek shows that there are 2,118 current job openings that specifically request GIAC certification holders. 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 sum, we foresee strong demand for at least 200 graduates per year, in Maryland alone, from our MSISE program. This aligns with the State Plan Goal #8 and with our STI Strategic Goal #1.

D. <u>Reasonableness of Program Duplication</u>:

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 significant 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.

Since MHEC authorized STI to award master’s programs, the MSISE program remains critical and importantly distinct from other programs in Maryland (and the nation):

a. The SANS Technology Institute builds on the technical training of the SANS Institute, which has trained more than 180,000 information security professionals and teachers since 1989. The SANS Institute is the largest cybersecurity training organization, serving the National Security Agency, the FBI, and the US military, as well as their counterparts in many U.S. allied nations. Intelligence, military, and law enforcement organizations account for approximately 20% of SANS students. Others come from more than 5,000 enterprises of all types, ranging from hospitals to banks, utilities, state governments, and churches. Well over 2,000 faculty members and cybersecurity staff from U.S. and international colleges and universities have attended SANS courses.
b. The SANS Technology Institute takes the deep technical instruction of the SANS Institute to an entirely new level. The MSISE program focuses on integrating that technical material into an enterprise view that enables its students to judge, prioritize, and justify alternative approaches to reducing risk—generally within the Critical Controls framework pioneered by STI and SANS and now adopted by the U.S. Department of Homeland Security and the British government’s Centre for the Protection of Critical Infrastructure.
c. Further, STI focuses on developing technical communications skills as well as project management skills essential for gaining support for technical cybersecurity programs and meeting management commitments. Because time away from work is very limited and individuals tend to focus their training on technical skills, it is uncommon for security practitioners to enroll in professional development courses. But these courses are essential for leadership positions, as one of STI’s students wrote in 2013:

> *“I have to admit that I would not have chosen the project management course if it were not in the STI curriculum, but I am quick to admit that it has helped me greatly at work. I apply a lot of the content at work each day, leading a multi-year, multi-million dollar program. I believe the*

stakeholder management and guarding against (future) stakeholder scope creep are my biggest takeaways from your course. You did a great job delivering the content and keeping the class engaged."

d. The integration of enterprise-level analysis, project management, writing, and presentation courses is only part of what makes the SANS Technology Institute and the MSISE program a fundamentally different experience. SANS is a training institution that imparts a tight package of skills and capabilities to students who rarely take more than one course every couple of years. In contrast, MSISE students participate in a clearly defined, integrated program of study and curricula over a multi-year period. The individual courses are powerful, but it is the integrated curricular experience provided by the SANS Technology Institute that produces enterprise-ready security leaders and practitioners. Through its thoughtful construction of "core" and elective paths, its focus not just on competency but on proficiency, and its progressive emphasis on applied research and written and verbal presentation skills, the SANS Technology Institute and the MSISE program integrate and augment SANS classes with its own courses and requirements into a whole greater than its constituent parts.

E. Relevance to 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.

F. Adequacy of Curriculum Design and Delivery to Related Learning Outcomes

1. Program Outline and Requirements

Required Courses in the MSISE Program

ISE 5101: Security Essentials
SANS class: SEC 401 Security Essentials Boot-camp Style
Assessment: GIAC GSEC
3 Credit Hours
ISE 5101 is the introductory, technically-oriented survey course in the information security engineering master's program. It 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 information security engineering master's program.

ISE 5201: Hacking Techniques & Incident Response
SANS class: SEC 504 Hacker Techniques, Exploits & Incident Handling
Assessment: GIAC GCIH
3 Credit Hours
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 class: MGT 433 Securing the Human: Building and Deploying an Effective Security Awareness Program
Assessment: Writing Exercise
1 Credit Hour
One of the most effective ways to secure the human factor in an enterprise is an active awareness and education program that goes beyond compliance and leads to actual changes in behaviors. In ISE 5300, students learn the key concepts and skills to plan, implement, and maintain an effective security awareness program that makes organizations both more secure and compliant. In addition, metrics are introduced to measure the impact of the program and demonstrate value. Finally, through a series of labs and exercises, students develop their own project and execution plan, so they can immediately implement a customized awareness program for their organization.

ISE 5401: Advanced Network Intrusion Detection & Analysis
SANS class: SEC503: Intrusion Detection In-Depth
Assessment: GIAC GCIA
3 Credit Hours
ISE 5401 delivers the technical knowledge, insight, and hands-on training you need to defend your network with confidence. You will learn about the underlying theory of TCP/IP and the most used application protocols, such as DNS and HTTP, so that you can intelligently examine network traffic for signs of an intrusion. You will get plenty of practice learning to master different open source tools like tcpdump, Wireshark, Snort, Bro, tshark, and SiLK. Daily hands-on exercises suitable for all experience levels reinforce the course book material so that you can transfer knowledge to execution.

ISE 5501: Technical Research & Communication Practicum
Assessment: Research Paper, Presentation
3 Credit Hours
ISE 5501 is a graduate-level research and presentation course in which students will identify, investigate, and analyze a problem in order to then write and present on their findings and practical solutions. Students will write a research paper interpreting the data collected and making recommendations for action. The research paper 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 then convert their written technical material into a persuasive oral presentation appropriate in an enterprise environment. Students engage in an iterative process, using research material written for a previous course, as a base from which to build and deliver a 40-minute presentation, typically given via an online webinar and potentially at a SANS Residential Institute/instructional event for exemplary presentations.

ISE 5600: IT Security Leadership Competencies
SANS class: MGT 514, days 3,4, and 5, IT Security Strategic Planning, Policy, and Leadership
Assessment: Writing Exercise
1 Credit Hour
ISE 5600 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 5700: Situational Response Practicum
Assessment: Oral Presentation, Writing Exercise
1 Credit Hour
In ISE 5700, a small group of students is given an information security scenario that is partly based on current events, and requires a broad knowledge of information security concepts. Their task is to evaluate the scenario and to recommend a course of action. This experience is a timed 24-hour event and culminates in a group written report and presentation at the end of the 24-hour preparation time.

ISE 5800: IT Security Project Management
SANS class: MGT 525 IT Project Management, Effective Communication, and PMP® Exam Prep
Assessment: GIAC GCPM
3 Credit Hours
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 PMP® 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 6300: NetWars Continuous Practicum
Assessment: NetWars Continuous
1 Credit Hour
In ISE 6300, students will complete an online training program, NetWars Continuous, 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 6001: Standards Based Implementation of Security
SANS class: SEC 566 Implementing and Auditing the Twenty Critical Security Controls
Assessment: GIAC GCCC
3 Credit Hours
Cybersecurity attacks are increasing and evolving so rapidly that is more difficult than ever to prevent and defend against them. ISE 6001 will help you to ensure that your organization has an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches. As threats evolve, an organization's security should too. Standards based implementation takes a prioritized, risk-based approach to security and shows you how standardized controls are the best way to block known attacks and mitigate damage from successful attacks.

ISE 5901: Advanced Technical Research & Communication Practicum
Assessment: Research Paper, Presentation
3 Credit Hours
ISE 5901 is a graduate-level research and presentation course in which students will identify, investigate, and analyze a problem in order to then write and present on their findings and practical solutions. Students will write a research paper interpreting the data collected and making recommendations for action. The research

paper 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 then convert their written technical material into a persuasive oral presentation appropriate in an enterprise environment. Students engage in an iterative process, using research material written for a previous course, as a base from which to build and deliver a 40-minute presentation, typically given via an online webinar and potentially at a SANS Residential Institute/instructional event for exemplary presentations.

ISE 6100: Security Project Practicum
Assessment: Group Written Project Plan
1 Credit Hour
In ISE 6100, a small group of students is given an information security project that requires a broad knowledge of information security concepts. Their task is to evaluate the project assignment and to recommend a course of action. This experience is a timed 30-day event. Students receive the project assignment from faculty, and must respond with a project plan to address the assignment within 5 days. The group then uses their plan to address the assignment, and deliver a written report at the end of the 30-day period**.**

ISE 7000: GIAC Security Expert Certification Technical Capstone
Assessment: GIAC Security Expert Certification Exam
1 Credit Hour
The GSE exam Capstone experience has two parts. The first is a multiple choice exam which may be taken at a proctored location just like any other GIAC exam. Passing this exam qualifies students to sit for the GSE hands-on lab. The first day of the two day GSE lab consists of an incident response scenario that requires the candidate to analyze data and report their results in a written report. The second consists of a rigorous battery of hands-on exercises drawn from a variety of information security domains.

Elective Courses (Three):

Students enrolled in the MSISE degree program must choose three different technical courses from among those listed below. Course choices may be designed to extend the breadth of a student's technical knowledge base, or may be focused all within a particular practice area of cybersecurity.

ISE 6215: Advanced Security Essentials
SANS class: SEC 501 Advanced Security Essentials - Enterprise Defender
Assessment: GIAC GCED
3 Credit Hours
ISE 6215 reinforces the theme that prevention is ideal, but detection is a must. Students will learn how to ensure that their organizations constantly improve their security posture to prevent as many attacks as possible. A key focus is on data protection, securing critical information no matter whether it resides on a server, in robust network architectures, or on a portable device.
Despite an organization's best effort at preventing attacks and protecting its critical data, some attacks will still be successful. Therefore students will also learn how to detect attacks in a timely fashion through an in-depth understanding the traffic that flows on networks, scanning for indications of an attack. The course also includes instruction on performing penetration testing, vulnerability analysis, and forensics.

ISE 6230: Securing Windows with the Critical Security Controls
SANS class: SEC 505 Securing Windows and PowerShell Automation
Assessment: GIAC GCWN
3 Credit Hours
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. This course applies the Critical Security Controls to Windows, so it is a natural follow-on to ISE 6000 (SEC566), which is a required course for the curriculum.

ISE 6235: Securing Linux/Unix
SANS class: SEC 506 Securing Linux/Unix
Assessment: GIAC GCUX
3 Credit Hours
ISE 6235 provides students with experience in in-depth coverage of Linux and Unix security issues, examining how to mitigate or eliminate general problems that apply to all Unix-like operating systems, including vulnerabilities in the password authentication system, file system, virtual memory system, and applications that commonly run on Linux and Unix. This course provides specific configuration guidance and practical, real-world examples, tips, and tricks.

ISE 6240: Continuous Monitoring and Security Operations
SANS class: SEC 511 Continuous Monitoring and Security Operations
Assessment: GIAC GMON
3 Credit Hours
ISE6240 teaches a proactive approach to enterprise security that presumes attackers will penetrate your environment and therefore emphasizes timely incident detection. The Defensible Security Architecture, Network Security Monitoring, Continuous Diagnostics and Mitigation, and Continuous Security Monitoring taught in this course - aligned with the National Institute of Standards and Technology (NIST) guidelines described in NIST SP 800-137 for Continuous Monitoring (CM) -- are designed to enable you and your organization to analyze threats and detect anomalies that could indicate cybercriminal behavior.

ISE 6315: Web App Penetration Testing and Ethical Hacking
SANS class: SEC 542 Web App Penetration Testing and Ethical Hacking
Assessment: GIAC GWAPT
3 Credit Hours
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 class: SEC 560 Network Penetration Testing and Ethical Hacking
Assessment: GIAC GPEN
3 Credit Hours
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
SANS class: SEC 575 Mobile Device Security and Ethical Hacking
Assessment: GIAC GMOB
3 Credit Hours
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
SANS class: SEC 617 Wireless Ethical Hacking, Penetration Testing, and Defenses
Assessment: GIAC GAWN
3 Credit Hours
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: Automating Information Security with Python
SANS class: SEC573: Automating Information Security with Python
Assessment: GIAC GPYC
3 Credit Hours
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
SANS class: SEC 660 Advanced Penetration Testing, Exploits, and Ethical Hacking
Assessment: GIAC GXPN
3 Credit Hours
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.

ISE 6420: Computer Forensic Investigations - Windows
SANS class: FOR 500: Windows Forensic Analysis
Assessment: GIAC GCFE
3 Credit Hours
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 Computer Forensic Analysis and Incident Response
SANS class: FOR 508 Advanced Digital Forensics, Incident Response, and Threat Hunting
Assessment: GIAC GCFA
3 Credit Hours
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 6445: Cyber Threat Intelligence
SANS class: FOR 578 Cyber Threat Intelligence
Assessment: GIAC GCTI
3 Credit Hours
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 6440: Advanced Network Forensics and Analysis
SANS class: FOR 572 Advanced Network Forensics and Analysis
Assessment: GIAC GNFA
3 Credit Hours
ISE 6440: Advanced Network Forensics and Analysis 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. Hands-on exercises in FOR 572 cover a wide range of open source and commercial tools, and real-world scenarios help the student learn the underlying techniques and practices to best evaluate the most common types of network-based attacks.

ISE 6450: Advanced Smartphone Forensics
SANS class: FOR585: Advanced Smartphone Forensics
Assessment: GIAC GASF
3 Credit Hours
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: Malware Analysis and Reverse Engineering
SANS class: FOR 610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques
Assessment: GIAC GREM
3 Credit Hours
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 class: ICS 410 ICS/SCADA Security Essentials
Assessment: GIAC GICSP
3 Credit Hours
ISE 6515 ICS/SCADA Security Essentials is an introductory study of how information technologies and operational technologies have converged in today's industrial control system environments. This convergence has led to a greater need than ever 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 class: ICS 515 ICS Active Defense and Incident Response
Assessment: GIAC GRID
3 Credit Hours
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.

ISE 6525: Essentials for NERC Critical Infrastructure Protection
SANS class: ICS 456 Essentials for NERC Critical Infrastructure Protection
Assessment: GIAC GCIP
3 Credit Hours
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 class: DEV 522 Defending Web Applications Security Essentials
Assessment: GIAC GWEB
3 Credit Hours
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 6715: Auditing Networks, Perimeters and Systems
SANS class: AUD 507 Auditing Networks, Perimeters, and Systems
Assessment: GIAC GSNA
3 Credit Hours
(Not available as an elective in the MSISM program)
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: Law of Data Security and Investigations
SANS class: LEG 523 Law of Data Security and Investigations
Assessment: GIAC GLEG
3 Credit Hours
(Not available as an elective in the MSISM program)
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.

The MSISE program provides for the option of a focus area for a student’s electives. It is not required that an MSISE student select focus area. Any student who does not select focus area is free to select any combination of available electives of their own choosing, and to receive the MSISE degree upon meeting graduation requirements. An MSISE student may declare into a focus area at any time.

A focus area consists of three electives designated within any of the below categories.

1. **Blue Team Operations**:

   a. ISE 6215: Advanced Security Essentials
      i. SANS class: SEC 501 Advanced Security Essentials - Enterprise Defender
      ii. Assessment: GIAC GCED

   b. ISE 6230: Securing Windows with the Critical Security Controls
      i. SANS class: SEC 505 Securing Windows and PowerShell Automation
      ii. Assessment: GIAC GCWN

   c. ISE 6235: Securing Linux/Unix
      i. SANS class: SEC 506 Securing Linux/Unix
      ii. Assessment: GIAC GCUX

   d. ISE 6240: Continuous Monitoring and Security Operations
      i. SANS class: SEC 511 Continuous Monitoring and Security Operations
      ii. Assessment: GIAC GMON

   e. ISE 6350: Automating Information Security with Python
      i. SANS class: SEC573: Automating Information Security with Python
      ii. Assessment: GIAC GPYC

2. **Penetration Testing**:

   a. ISE 6315: Web App Penetration Testing and Ethical Hacking
      i. SANS class: SEC 542 Web App Penetration Testing and Ethical Hacking
      ii. Assessment: GIAC GWAPT

   b. ISE 6320: Network Penetration Testing and Ethical Hacking
      i. SANS class: SEC 560 Network Penetration Testing and Ethical Hacking
      ii. Assessment: GIAC GPEN

   c. ISE 6325: Mobile Device Security
      i. SANS class: SEC 575 Mobile Device Security and Ethical Hacking
      ii. Assessment: GIAC GMOB

   d. ISE 6330: Wireless Penetration Testing
      i. SANS class: SEC 617 Wireless Ethical Hacking, Penetration Testing, and Defenses
      ii. Assessment: GIAC GAWN

   e. ISE 6350: Automating Information Security with Python
      i. SANS class: SEC573: Automating Information Security with Python
      ii. Assessment: GIAC GPYC

   f. ISE 6360: Advanced Penetration Testing
      i. SANS class: SEC 660 Advanced Penetration Testing, Exploits, and Ethical Hacking
      ii. Assessment: GIAC GXPN

3. **Digital Forensics and Incident Response**:

   a. ISE 6420: Computer Forensic Investigations - Windows
      i. SANS class: FOR 500: Windows Forensic Analysis
      ii. Assessment: GIAC GCFE

   b. ISE 6425: Advanced Computer Forensic Analysis and Incident Response
      i. SANS class: FOR 508 Advanced Digital Forensics, Incident Response, and Threat Hunting

        ii. Assessment: GIAC GCFA
    c. ISE 6440: Advanced Network Forensics and Analysis
        i. SANS class: FOR 572 Advanced Network Forensics and Analysis
        ii. Assessment: GIAC GNFA
    d. ISE 6445: Cyber Threat Intelligence
        i. SANS class: FOR 578 Cyber Threat Intelligence
        ii. Assessment: GIAC GCTI
    e. ISE 6450: Advanced Smartphone Forensics
        i. SANS class: FOR585: Advanced Smartphone Forensics
        ii. Assessment: GIAC GASF
    f. ISE 6460: Malware Analysis and Reverse Engineering
        i. SANS class: FOR 610 Reverse-Engineering Malware: Malware Analysis Tools and Techniques
        ii. Assessment: GIAC GREM

4. **Security Management and Policy**:

    a. ISE 6720: Law of Data Security and Investigations
        i. SANS class: LEG 523 Law of Data Security and Investigations
        ii. Assessment: GIAC GLEG
    b. ISE 6715: Auditing Networks, Perimeters and Systems
        i. SANS class: AUD 507 Auditing Networks, Perimeters, and Systems
        ii. Assessment: GIAC GSNA
    c. One additional elective of the student's choosing

5. **Industrial Control Systems**:

    a. ISE 6515: ICS/SCADA Security Essentials
        i. SANS class: ICS 410 ICS/SCADA Security Essentials
        ii. Assessment: GIAC GICSP
    b. ISE 6525: Essentials for NERC Critical Infrastructure Protection
        i. SANS class: ICS 456 Essentials for NERC Critical Infrastructure Protection
        ii. Assessment: GIAC GCIP
    c. ISE 6520: ICS Active Defense and Incident Response
        i. SANS class: ICS 515 ICS Active Defense and Incident Response
        Assessment: GIAC GRID

2. 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.
- Since 2014, we have added two additional program learning outcomes:
- 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.

3. How General Education Requirements Will Be Met

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

4. Specialized Accreditation/Certification Requirements

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

5. 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.

G. 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.

H. Adequacy of faculty resources (as outlined in COMAR 13B.02.03.11).

1. Provide a brief narrative demonstrating the quality of program faculty. Include a summary list of faculty with appointment type, terminal degree title and field, academic title/rank, status (full-time, part-time, adjunct) and the course(s) each faulty member will teach (in this program).

STI appoints its teaching faculty from the corps of instructors that are chosen and designated by the SANS Institute to teach its courses as Certified Instructors, Senior Instructors, Principal Instructors, and Fellows. Meeting STI's mission requires that STI faculty and graduates are "scholar-practitioners." STI uses the term "scholar-practitioner" to designate people who are both (1) highly trained professional practitioners focused on information security, and (2) scholars in the sense that they both contribute to and consume the research required to advance that professional practice. The combination enables them to incorporate new research into their work and create the new knowledge and solutions that others seek to use. Our faculty are not solely scholars, they must also be advanced practitioners of the subjects they teach so that they can show STI students how to practice security effectively. This gives STI students an advantage relative to graduates of other programs in which students learn theory, but not up-to-date practice. Finally, our faculty must be talented teachers, able to communicate often-difficult technical information in a clear and compelling manner.

Among STI's 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.

STI's faculty and leadership have earned significant general and industry recognition for their roles and expertise. To list just a few:

- President Alan Paller was the Co-chair of the Department of Homeland Security's Task Force on CyberSkills, and had been a Charter Member of President Clinton's National Information Assurance Council.
- President Paller, Dr. Eric Cole, and James Lyne are three of fewer than 30 people currently listed on the Infosecurity Europe Hall of Fame.
- Dr. Johannes Ullrich was recognized as one of the 50 most powerful people in networking by NetworkWorld. Social media is replete with examples of references to SANS Instructors, including items like Security Leaders to Follow on Social Media.

- STI faculty are repeatedly invited to keynote presence at RSA, the industry's largest convocation for information security research and practice. For each of the last seven years, members of STI's faculty, led by President Alan Paller, have hosted one of the main keynotes at "RSA," focusing their presentation on their expectations for the seven most dangerous new attack techniques they expect to impact the industry in the subsequent year. The press release regarding the entire event issued by RSA is indicative of our faculty's prominence in the industry: not only are they one of the three keynotes highlighted (together with a Cryptographer's panel, which is the core activity of RSA), but they are presented prior to and in advance of the CEOs, Presidents, and leading executives from companies such as Microsoft, Hewlett Packard Enterprise, Symantec, Intel Security, and Cisco Security.
- STI faculty are sought after by the news media for their commentary on cybersecurity topics – STI faculty are frequently sought-after as commentators for breaking news articles on adverse cyber events. Their commentary appears in general news publications such as the New York Times and Wall Street Journal, in general magazines such as Forbes and Fortune, and their work is highlighted on various TV news programs. They are sought-after speakers even for general industry events, such as TED (James Lyne's February, 2013 TED talk on 'everyday cybercrime' has been viewed 1.5mm times).

As shown in Figure 1 (below), the SANS instructor development and assessment process requires a prospective STI faculty member to successfully complete four increasingly competitive steps (listed here and described in greater detail below):

(1) Earn scores on a Global Information Assurance Certification (GIAC) examination above 85.
(2) Earn high marks in mentoring (lab/teaching assistant) two groups of students.
(3) Earn high marks as "community instructors" in teaching two classes held at small Residential Institutes.
(4) Earn high marks as a supervised instructor at a large Residential Institute.

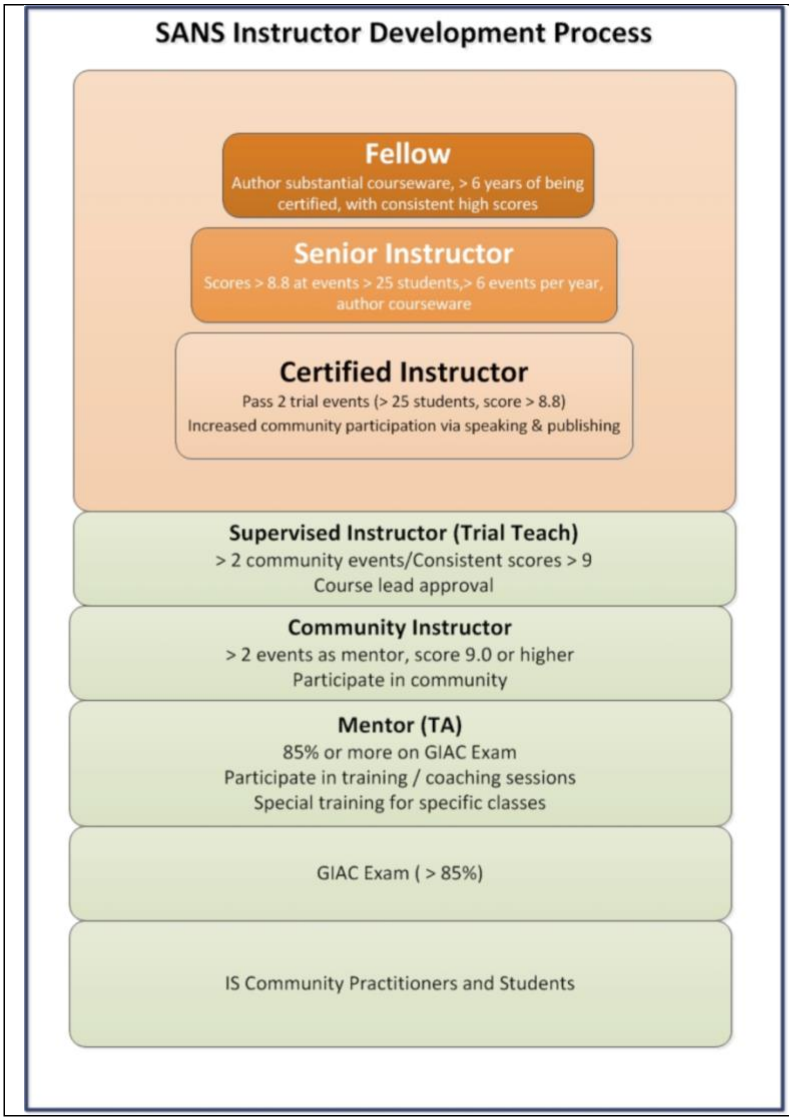
Only after completing these four steps would an individual would be eligible to be a SANS Certified Instructor and potentially be appointed to the STI faculty.

In the first step, teaching candidates are recruited from practitioners who score 85 or higher on the GIAC exam(s) relevant to the course(s) they will train to instruct. If selected, teaching candidates begin as designated SANS mentors and are then monitored and coached as they begin helping students who use online resources for instruction but look to SANS mentors for help with the lab exercises. The mentor stage in the SANS instructor development pipeline parallels the role of lab/teaching assistant in many college settings. Mentoring allows teaching candidates to develop and demonstrate their ability to coach students, demonstrate solutions to many hands-on exercises, and clarify the more challenging concepts being discussed in the courses. Students rank mentors on teaching skill and overall effectiveness, which allows SANS to determine whether the mentor is sufficiently talented to move on to the next step.

Mentors who earn outstanding scores in two separate 12-week mentoring assignments may then advance to the second step: closely monitored teaching engagements at small, community-based learning events (10-25 students), where they are designated as "community instructors."

Instructional effectiveness scores, part of the course evaluation process used for every teaching session delivered by SANS, are used to evaluate each instructor's ability to teach, as well as to measure the teacher's continued mastery of the material. Candidates who earn outstanding scores in effectiveness and satisfaction in two separate six-day community-teaching opportunities are invited to be guest instructors at a larger learning event. Those who earn outstanding scores at the larger event are designated as Certified Instructors.

Figure 1 SANS Instructor Development and Assessment Process


SANS Instructor Development Process
Fellow
Author substantial courseware, > 6 years of being certified, with consistent high scores
Senior Instructor
Scores > 8.8 at events > 25 students,> 6 events per year, author courseware
Certified Instructor
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

Typical numbers reaching each level in the faculty development pipeline, annually:

2 new fellows

4 new senior instructors

11 new certified instructors

15 new trial instructors

32 new community instructors

60 selected to mentor a course

5,000+ mentor-eligible GIAC test scores out of 12,000 who passed GIAC exams

The numbers on the right side of Figure 1 demonstrate the select nature of an STI faculty member. Fewer than half of more than 12,000 persons who take and pass GIAC information security certification exams each year are even eligible to become SANS mentors. Because of increasingly stringent class size and ratings requirements, the number of people who are promoted to each higher rank of teaching decreases as you go up the ladder. Thus, certified SANS instructors represent approximately 1 in 800 (15 selected out of 12,000) of the practitioners talented enough to pass GIAC exams. As importantly, SANS instructors retain their positions only if their ratings on course value (reflecting in part the currency and applicability of the examples used) and teaching effectiveness, which are recorded for every teaching engagement, remain above a high cutoff point (4.1 on a scale of 5). They must also remain ahead of other candidates coming up through the instructor development pipeline.

Once appointed, qualified individuals serve in dual roles as SANS Instructors and STI faculty members. Each appointed instructor is a proven, real-world practitioner whose experiences are especially relevant to the school, enabling them to author courses of value, relevancy, and currency, as well as to deliver these courses to students in an effective, highly engaging manner that includes supplying ever-renewed examples from their work practice. These industry-recognized demarcations indicate technical achievement 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.

While a handful of faculty members serve in full-time teaching and research roles, most are adjunct, scholar-practitioners who teach less than full-time for the school or our parent, SANS, 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, especially as it pertains to the MSISE program, includes the following individuals:

Dr. Johannes Ullrich – Dean of Research

Dr. Ullrich 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 – Dean of Faculty

David Hoelzer serves as the Dean of Faculty at STI, and is the author of large sections within four courses within the MSISE program. 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 – MSISE Program Director

Tim Medin serves as 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 a 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.

A summary list of MSISE faculty is available in Appendix 3.

The full listing of STI faculty, in all programs, can be found on our website at https://www.sans.edu/academics/faculty.

Ongoing Pedagogy Training for Faculty:

2. Demonstrate how the institution will provide ongoing pedagogy training for faculty in evidenced-based best practices, including training in:
a) Pedagogy that meets the needs of the students
b) The learning management system
c) Evidenced-based best practices for distance education, if distance education is offered.
Instructional pedagogy is an ingrained element of the SANS instructor developmental program, from which STI draws its faculty, and is reinforced during live teaching engagements and routinely during Curriculum Lead meetings. This instructional process is then continued on a recurring basis for new and current faculty members.

The SANS development and continuous assessment process ensures that persons eventually chosen to teach STI students demonstrate (1) mastery in the community of practice in which they instruct, and (2) highly rated and effective teaching practices. An equally important element of teaching quality at STI is that SANS' ongoing assessment processes enable the college to ensure that teaching faculty retain both a high degree of technical mastery and outstanding teaching skills on an ongoing basis.

During and after live teaching engagements, academic leadership and senior staff are provided with daily surveys of teaching effectiveness and subsequent aggregated reports. These include:

- Daily Reports, email to faculty and senior staff: With each day's survey scores from students, plus all written feedback comments, with highlights of positive and negative items. These daily reports enable overnight corrections to an adverse course experience or instructor performance
- Quarterly summaries: Including heat maps for 'success rates' by course
- Instructor reports: Success rate charts for all instructors, and faculty "ranking" by feedback measures

These reports not only demonstrate the ongoing, continual assessments performed by faculty leadership, to include the Curriculum Leads (more below on this position), they further provide timely and recurring opportunities to reinforce best practices and institutional pedagogy. While these data are distributed and reviewed each day, analysis of the quarterly summaries and comparison reports generates recognition of longer-term issues, opportunities for further faculty development, and required corrective actions.

Curriculum Leads, who act as the equivalent of "Department Heads" both for SANS and STI, play an important role in the management and development of other faculty. They are thought leaders individually, but they are also charged with the oversight of all courses within their curriculum, and meet as a group twice per year to review their curricula and pedagogy with each other. Individual faculty with identified performance issues, as highlighted on these quality assessment reports, are engaged by Curriculum Leads for further investigation and instruction.

Finally, our Dean of Faculty, David Hoelzer, personally conducts quarterly in-person pedagogy refresher training. During this two-day session, held in the evenings after the completion of classes for the day, faculty receive instruction on best practices in teaching, presentation style, the conduct of labs, and engagement with students. This training is mandatory for new faculty, is open to all faculty, and occasionally involves a direct invitation to a current faculty member who, by virtue of the daily teaching assessment process described above, is deemed as able to benefit from refresher training. As a new initiative this year, these quarterly pedagogy training sessions are being supplemented by separate, additional sessions presented by Ed Skoudis, the Curriculum Lead for Penetration Testing. These supplemental sessions provide current instructors with expert and current practices for incorporating story-telling into their classroom presentation style.

LMS and Distance Education Training for Faculty:

The MSISE program uses the same combination of live classroom and three distance learning modalities used in the STI graduate program that was commended for its "creative and forward looking teaching methodology" in the April 2018 Team Report to the Middle States Commission on Higher Education.

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.

Faculty who teach through our OnDemand, vLive and Simulcast modalities undergo specific training to help modify their teaching style to this format. STI faculty, who author all course content, are then supported by a dedicated team of online learning subject matter experts who maintain and monitor our learning management system. We engage this team of online learning experts to assist in both (1) the recording of distance learning course content and (2) online-specific methods to enable virtual student-faculty interactions, including when a class is Simulcast to remote students, employing an assistant in the room who participates in the class on behalf of distance students by flagging the instructors attention when questions or issues are addressed by virtual students. Members of the faculty have developed guidelines for best practices when teaching in our distance education formats. Thus, our design and delivery model distinguishes clearly between activities meant to be carried out by faculty, and those that are optimally conducted by dedicated, full-time staff.

All courses are reviewed annually for possible minor updates, and once every three years for major updates. During those reviews, faculty work with the LMS and distance learning subject matter experts to adjust both content and delivery in order to align with current best practices. STI uses this course evaluation process for ongoing internal and external effectiveness assessments to monitor (1) learner satisfaction, (2) applicability and value of material being taught, (3) alignment of methods with the community of practice, and (4) faculty performance. During or immediately following each learning experience, students are asked to provide feedback on the faculty and the course content, and these evaluations are available to instructors who may review them each evening. Assessment analysts aggregate the data from the evaluations and feedback after every learning event, creating an event report which is reviewed by important stakeholders, including the program directors, members of the Curriculum, Academic, Faculty and Student Affairs Committee, and STI's President. Potential problems, generally identified by scores falling below a threshold in one or more areas are investigated by members of the Curriculum, Academic, Faculty and Student Affairs Committee with responsibility for overseeing curriculum within a cognate discipline. When required, this allows for real-time remediation of any shortfalls in pedagogy or delivery of content.

For evidenced-based best practices for faculty use of our learning management systems and distance education, see Appendix 2. "Evidence of Compliance with the Principles of Good Practice (outlined in COMAR 13B02.03.22C)."

I. <u>Adequacy of Library Resources</u> (as outlined in COMAR 13B.02.03.12).

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, new technologies that are emerging, and analysis of security trends.

J. Adequacy of Physical Facilities, Infrastructure and Instructional Equipment (as outlined in COMAR 13B.02.03.13)

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.

K. Adequacy of Financial Resources with Documentation (as outlined in COMAR 13B.02.03.14)

1. *Complete Table 1: Resources (pdf) and Table 2: Expenditure(pdf). Finance data(pdf) for the first five years of program implementation are to be entered. Figures should be presented for five years and then totaled by category for each year.*
2. *Provide a narrative rationale for each of the resource categories. If resources have been or will be reallocated to support the proposed program, briefly discuss the sources of those funds.*

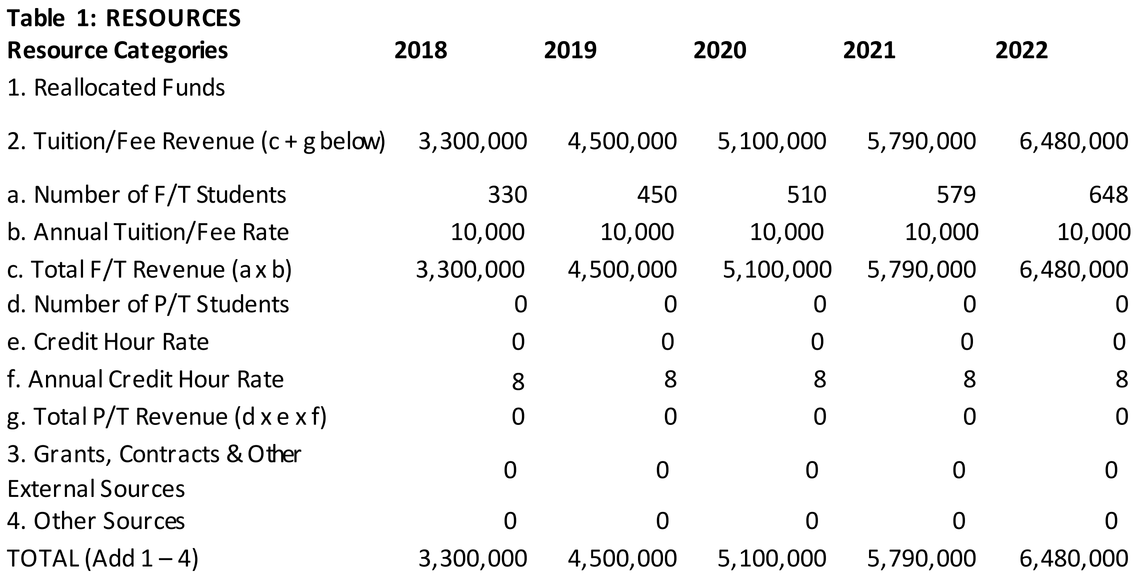


Table 1: RESOURCES

Resource Categories	**2018**	**2019**	**2020**	**2021**	**2022**
1. Reallocated Funds					
2. Tuition/Fee Revenue (c + g below)	3,300,000	4,500,000	5,100,000	5,790,000	6,480,000
a. Number of F/T Students	330	450	510	579	648
b. Annual Tuition/Fee Rate	10,000	10,000	10,000	10,000	10,000
c. Total F/T Revenue (a x b)	3,300,000	4,500,000	5,100,000	5,790,000	6,480,000
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)	3,300,000	4,500,000	5,100,000	5,790,000	6,480,000

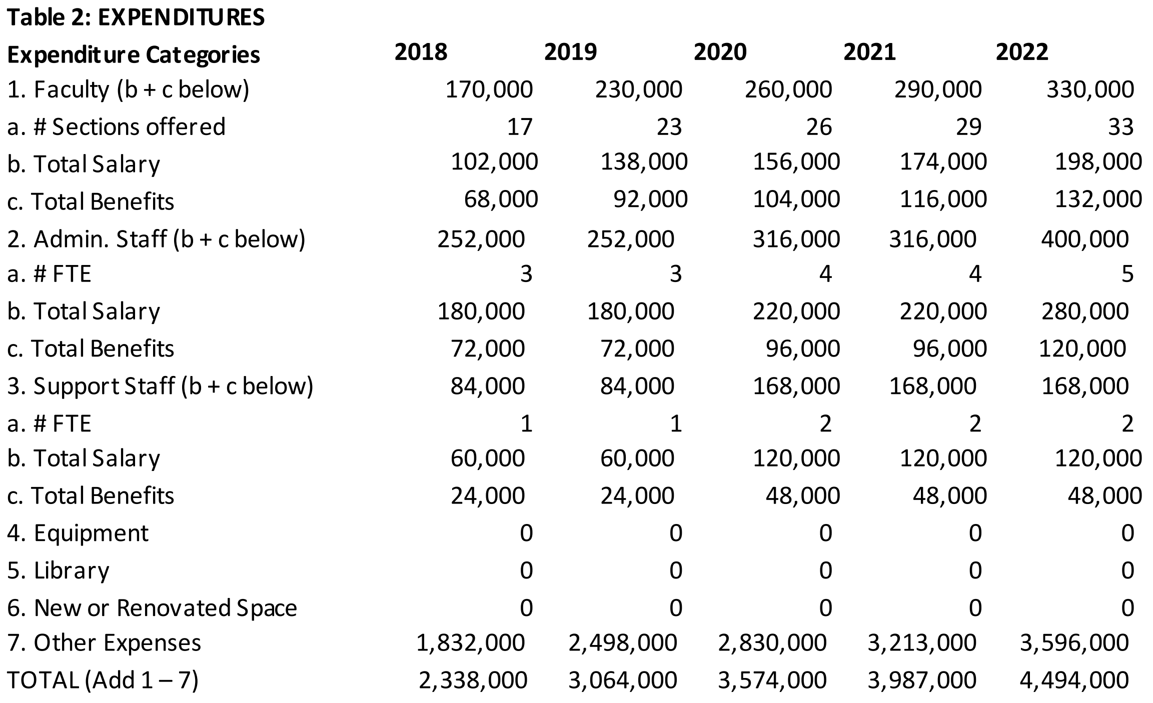


Table 2: EXPENDITURES

Expenditure Categories	**2018**	**2019**	**2020**	**2021**	**2022**
1. Faculty (b + c below)	170,000	230,000	260,000	290,000	330,000
a. # Sections offered	17	23	26	29	33
b. Total Salary	102,000	138,000	156,000	174,000	198,000
c. Total Benefits	68,000	92,000	104,000	116,000	132,000
2. Admin. Staff (b + c below)	252,000	252,000	316,000	316,000	400,000
a. # FTE	3	3	4	4	5
b. Total Salary	180,000	180,000	220,000	220,000	280,000
c. Total Benefits	72,000	72,000	96,000	96,000	120,000
3. Support Staff (b + c below)	84,000	84,000	168,000	168,000	168,000
a. # FTE	1	1	2	2	2
b. Total Salary	60,000	60,000	120,000	120,000	120,000
c. Total Benefits	24,000	24,000	48,000	48,000	48,000
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	1,832,000	2,498,000	2,830,000	3,213,000	3,596,000
TOTAL (Add 1 – 7)	2,338,000	3,064,000	3,574,000	3,987,000	4,494,000

Finance Data: Narrative

Table 1: RESOURCES

1. Re-allocated Funds

Narrative: Analyze the overall impact that the reallocation will have on the institution, particularly on existing programs and organizations units.

N/A

2. Tuition and Fee Revenue

Narrative: Describe the rationale for the enrollment projections used to calculate tuition and fee revenue.

The tuition projection for 2018 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.

3. Grants and Contracts

Narrative: Provide detailed information on the sources of funding. Attach copies of documentation supporting funding. Also, describe alternative methods of continuing to finance the program after outside funds cease to be available.

N/A

4. Other Sources

Narrative: Provide detailed information on the sources of the funding, including supporting documentation.

N/A

5. Total Year

Narrative: Additional explanation or comments as needed.

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.

L. <u>Adequacy of Provisions for Evaluation of Program</u> (as outlined in COMAR 13B.02.03.15).

Discuss procedures for evaluating courses, faculty and student learning outcomes.

Faculty at STI oversees a learning outcomes assessment process that occurs throughout a student's experience. STI's Curriculum Committee, supported by the Faculty and Research sub-committees, provides oversight of the assessment process to ensure that students are mastering the appropriate program learning outcomes by reviewing quarterly performances on exams, research papers, alternative written assignments, projects and presentations. In addition to helping ensure that students master their program learning outcomes, results from learning assessments are also used to ensure the curriculum is aligned with the community of practice and meets the needs and expectations of our students, their employers, established industry and school standards, and our STI mission.

Eighteen types of direct and indirect assessment measures are used to assess student learning: daily course surveys, GIAC exam scores, research paper scores, presentation scores, group project scores, annual student survey, graduate exit surveys, and alumni surveys. Results from assessments are used in program and curriculum assessment as per our STI Learning Outcomes Assessment Plan.

STI relies on course evaluations to determine curriculum alignment with communities of practice as well as the quality of instruction. Because students are mid-level professionals, most classes include some students with advanced knowledge of relevant areas of security practice. Courses are evaluated by thousands of SANS students as well as STI students, and their combined daily feedback on course currency, accuracy, and utility provides a continuous flow of assessment data directly useful to course authors in ensuring their courses reflect current best practices. The course evaluation process is an integral component of institutional effectiveness. At the conclusion of each day of instruction, students are asked to evaluate their instructor, the learning environment, and the overall learning experience. Evaluations are preliminarily reviewed during the learning event to allow for immediate changes in the learning environment. After each learning event, evaluations are analyzed by SANS assessment analysts. An event report is generated and provided to all stakeholders, including the course author, instructor, and STI's President. STI faculty use results from learning events along with data from GIAC exam assessments to make updates to the curriculum as needed.

STI consolidated these various assessment activities into its strategic Learning Outcomes Assessment Plan, as presented to MHEC and MSCHE in our recent self-study report, and as specifically noted for approval in the MSCHE evaluation team report.

M. Consistency with the State's minority student achievement goals (as outlined in COMAR 13B.02.03.05 and in the State Plan for Postsecondary Education).

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.

N. Relationship to low productivity programs identified by the Commission

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

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.

Two Memoranda of Understanding (MOU) define the business relationships between STI, its SANS parent, and its sister organization the Global Information Assurance Certification (GIAC) organization. Those MOUs are reproduced in full below.

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 faculty and lab instruction in a high-quality fashion	SANS Institute will make available all performance ratings derived 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 Cont	$ 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 Cont	$ 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

SANS Technology Institute-GIAC Memorandum of Understanding

Agreement Published Date: January 1, 2018

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

Contents

Purpose

This Memorandum of Understanding ("MOU") revises and supersedes any previously signed agreement between the SANS Technology Institute (STI) and Global Information Assurance Certification (GIAC). This MOU:

- outlines services to be offered and working assumptions between STI and GIAC;
- quantifies and measures service level expectations;
- outlines the potential methods used to measure the quality of service provided;
- defines mutual requirements and expectations for critical processes and overall performance;
- strengthens communication between the provider of assessment services (GIAC) and its enterprise customer (STI);
- provides a vehicle for resolving conflicts.

Vision

GIAC will provide student assessment services for the STI enterprise. The primary goals for the MOU include:

- **Provide** access to high quality services for students, community and faculty, while ensuring identity and examination integrity in a secure and test-friendly environment.
- **Provide** meaningful certification services to students while promoting their academic, career and personal goals.
- **Demonstrate** that STI students can contribute to the knowledge base in information security and can communicate that knowledge to key communities of interest in information security.

Mission

Through various service units, GIAC provides assessment 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

GIAC shall provide job task analysis-based assessments in the form of proctored certification exams.

Hours of Operations

Through the use of technology and GIAC directed service providers, it is expected that assessment services provided will be available to STI students on a 24-hour basis.

Service Expectations

STI and GIAC 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 GIAC. The productivity indicators reflected below are not listed in any order of priority.

Process	Service Expectation	Service Metric
Certification Examinations		
Exam preparation	Provide access to two practice exams	Practice exams will be available to students within 10 days of exam registration
Test center experience	Students will be provided a professional environment free of distractions for taking exams	Test center experiences will receive an average rating of at least 4 out of 5 on an annual student survey
Quality management of examination	Exam will maintain their relevance to the job field for which they are certifying	All GIAC exams given will receive a rating of acceptable in their validation reports.
Supply of data for STI program assessment	GIAC will supply STI with exam results for further evaluation	GIAC will supply STI with individual and collective performance reports on a quarterly basis, or as required.

Service Constraints

- ***Scheduling of Capstone Examinations*** **-** The scheduling of the capstone GSE and GSM examinations will occur in conjunction with appropriate STI administrative staff and will adequately account for the number of students requiring a given capstone examination during each year.
- ***Conformance Requirements*** **-** ANSI policy changes may alter procedures and service delivery timeframes.
- ***Dependencies*** **-** Achievement of the service level commitment is dependent upon student and faculty compliance with the policies and procedures of GIAC.

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 GIAC will jointly conduct periodic reviews of individual GIAC assessment 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 GIAC 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 Director of GIAC 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 GIAC according to the following schedule:

- STI will pay GIAC $325 each time a student pays for a GIAC exam as part of their program of studies, or when they pay tuition or pay for credit hours for a course in which they will take a GIAC certification exam.
- STI will specifically pay GIAC $1000 each time a student pays for a GSE or GSM exam as part of their program of studies.

Agreed to on behalf of STI:	Agreed to on behalf of GIAC:
______________________________	________________________________
Eric A. Patterson Executive Director SANS Technology Institute	Scott Cassity Executive Director GIAC
______________________________	________________________________
Date	Date

Appendix 2. Evidence of Compliance with the Principles of Good Practice (outlined in COMAR 13B02.03.22C)

The proposed program uses the same combination of live classroom and three distance learning modalities used in the STI graduate program that 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.

(a) Curriculum and instruction

(i) 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,

(ii) 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, we 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

(iii) 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 MSISE 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.

(iv) 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.

(v) 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.

(b) Role and mission

(i) 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.

(ii) 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.

(c) Faculty support

(i) 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.

(ii) 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 ("Before we move on, are there any questions from our remote students?").

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. 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.

22. 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.
23. 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.

(iii) 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.

(d) 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.

(e) Students and student services

(i) 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 STI 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. For example, for ISE 5201: Incident Handling and Hacker Exploits, the corresponding course site at SANS (https://www.sans.org/course/hacker- techniques-exploits-incident-handling) provides detailed technical requirements as well as a tech support contact to help students ensure they have the right equipment and software versions.

- 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

(ii) 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.2.2).

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%

(iii) 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.

(iv) Advertising, recruiting, and admissions materials shall clearly and accurately represent the program, and the services available

Advertising, recruiting, and admissions materials for MSISE students were available in the Resource Room during our recent MSCHE and MHEC evaluation team visit. 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.

(f) Commitment to support

(i) 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.

(ii) 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 continue to deliver the MSISE program.

(g) Evaluation and assessment

(i) 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." This same system will be continue to be used in the distance learning components of the MSISE program

(ii) 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.

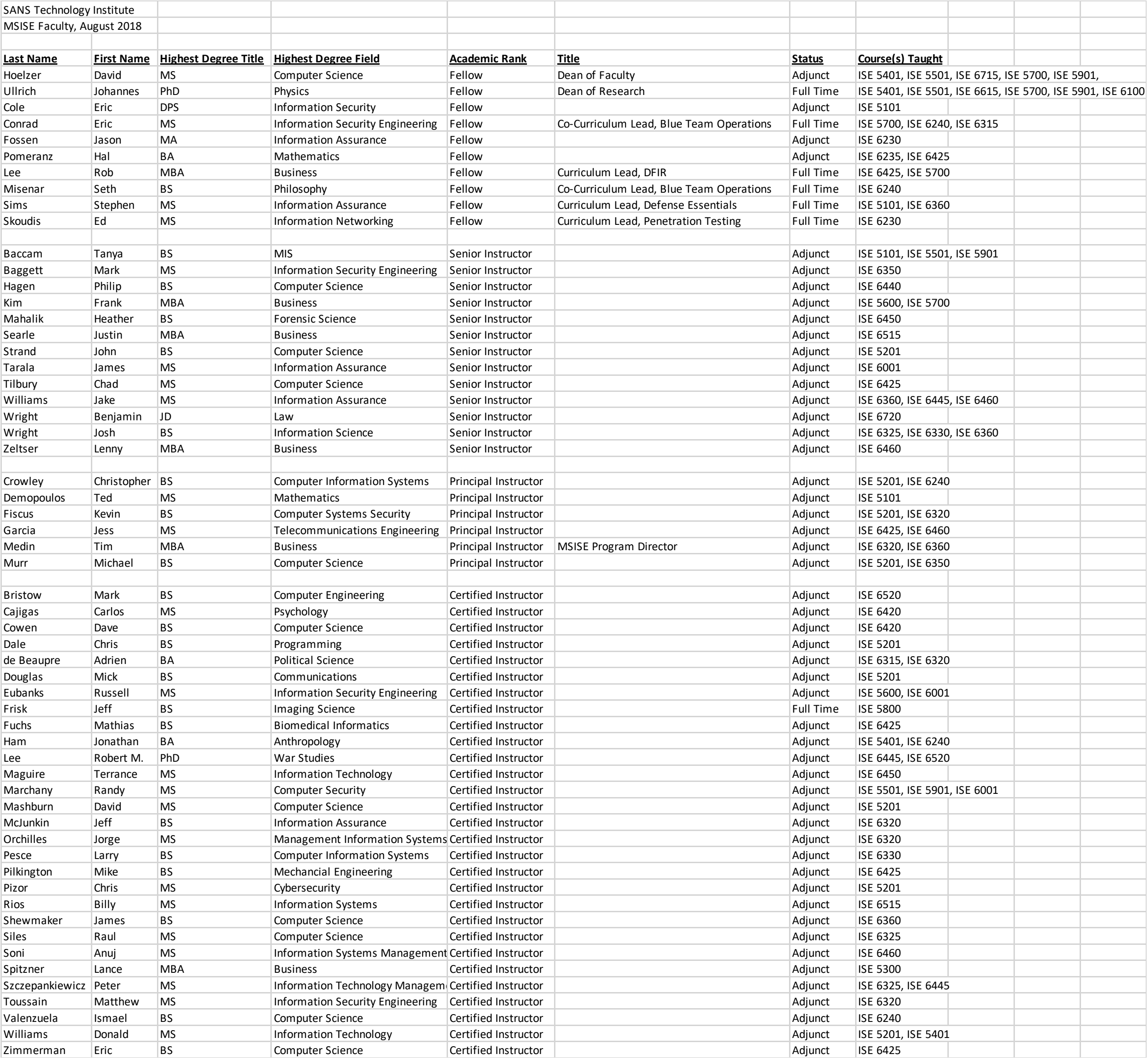
(iii) An institution shall provide for assessment and documentation of student achievement of learning outcomes in a distance education program.

Ultimate student achievement in the MSISE program will continue to 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.2.3, 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

Appendix 3. Summary Listing of MSISE Faculty



SANS Technology Institute

MSISE Faculty, August 2018

Last Name	First Name	Highest Degree Title	Highest Degree Field	Academic Rank	Title	Status	Course(s) Taught
Hoelzer	David	MS	Computer Science	Fellow	Dean of Faculty	Adjunct	ISE 5401, ISE 5501, ISE 6715, ISE 5700, ISE 5901,
Ullrich	Johannes	PhD	Physics	Fellow	Dean of Research	Full Time	ISE 5401, ISE 5501, ISE 6615, ISE 5700, ISE 5901, ISE 6100
Cole	Eric	DPS	Information Security	Fellow		Adjunct	ISE 5101
Conrad	Eric	MS	Information Security Engineering	Fellow	Co-Curriculum Lead, Blue Team Operations	Full Time	ISE 5700, ISE 6240, ISE 6315
Fossen	Jason	MA	Information Assurance	Fellow		Adjunct	ISE 6230
Pomeranz	Hal	BA	Mathematics	Fellow		Adjunct	ISE 6235, ISE 6425
Lee	Rob	MBA	Business	Fellow	Curriculum Lead, DFIR	Full Time	ISE 6425, ISE 5700
Misenar	Seth	BS	Philosophy	Fellow	Co-Curriculum Lead, Blue Team Operations	Full Time	ISE 6240
Sims	Stephen	MS	Information Assurance	Fellow	Curriculum Lead, Defense Essentials	Full Time	ISE 5101, ISE 6360
Skoudis	Ed	MS	Information Networking	Fellow	Curriculum Lead, Penetration Testing	Full Time	ISE 6230
Baccam	Tanya	BS	MIS	Senior Instructor		Adjunct	ISE 5101, ISE 5501, ISE 5901
Baggett	Mark	MS	Information Security Engineering	Senior Instructor		Adjunct	ISE 6350
Hagen	Philip	BS	Computer Science	Senior Instructor		Adjunct	ISE 6440
Kim	Frank	MBA	Business	Senior Instructor		Adjunct	ISE 5600, ISE 5700
Mahalik	Heather	BS	Forensic Science	Senior Instructor		Adjunct	ISE 6450
Searle	Justin	MBA	Business	Senior Instructor		Adjunct	ISE 6515
Strand	John	BS	Computer Science	Senior Instructor		Adjunct	ISE 5201
Tarala	James	MS	Information Assurance	Senior Instructor		Adjunct	ISE 6001
Tilbury	Chad	MS	Computer Science	Senior Instructor		Adjunct	ISE 6425
Williams	Jake	MS	Information Assurance	Senior Instructor		Adjunct	ISE 6360, ISE 6445, ISE 6460
Wright	Benjamin	JD	Law	Senior Instructor		Adjunct	ISE 6720
Wright	Josh	BS	Information Science	Senior Instructor		Adjunct	ISE 6325, ISE 6330, ISE 6360
Zeltser	Lenny	MBA	Business	Senior Instructor		Adjunct	ISE 6460
Crowley	Christopher	BS	Computer Information Systems	Principal Instructor		Adjunct	ISE 5201, ISE 6240
Demopoulos	Ted	MS	Mathematics	Principal Instructor		Adjunct	ISE 5101
Fiscus	Kevin	BS	Computer Systems Security	Principal Instructor		Adjunct	ISE 5201, ISE 6320
Garcia	Jess	MS	Telecommunications Engineering	Principal Instructor		Adjunct	ISE 6425, ISE 6460
Medin	Tim	MBA	Business	Principal Instructor	MSISE Program Director	Adjunct	ISE 6320, ISE 6360
Murr	Michael	BS	Computer Science	Principal Instructor		Adjunct	ISE 5201, ISE 6350
Bristow	Mark	BS	Computer Engineering	Certified Instructor		Adjunct	ISE 6520
Cajigas	Carlos	MS	Psychology	Certified Instructor		Adjunct	ISE 6420
Cowen	Dave	BS	Computer Science	Certified Instructor		Adjunct	ISE 6420
Dale	Chris	BS	Programming	Certified Instructor		Adjunct	ISE 5201
de Beaupre	Adrien	BA	Political Science	Certified Instructor		Adjunct	ISE 6315, ISE 6320
Douglas	Mick	BS	Communications	Certified Instructor		Adjunct	ISE 5201
Eubanks	Russell	MS	Information Security Engineering	Certified Instructor		Adjunct	ISE 5600, ISE 6001
Frisk	Jeff	BS	Imaging Science	Certified Instructor		Full Time	ISE 5800
Fuchs	Mathias	BS	Biomedical Informatics	Certified Instructor		Adjunct	ISE 6425
Ham	Jonathan	BA	Anthropology	Certified Instructor		Adjunct	ISE 5401, ISE 6240
Lee	Robert M.	PhD	War Studies	Certified Instructor		Adjunct	ISE 6445, ISE 6520
Maguire	Terrance	MS	Information Technology	Certified Instructor		Adjunct	ISE 6450
Marchany	Randy	MS	Computer Security	Certified Instructor		Adjunct	ISE 5501, ISE 5901, ISE 6001
Mashburn	David	MS	Computer Science	Certified Instructor		Adjunct	ISE 5201
McJunkin	Jeff	BS	Information Assurance	Certified Instructor		Adjunct	ISE 6320
Orchilles	Jorge	MS	Management Information Systems	Certified Instructor		Adjunct	ISE 6320
Pesce	Larry	BS	Computer Information Systems	Certified Instructor		Adjunct	ISE 6330
Pilkington	Mike	BS	Mechancial Engineering	Certified Instructor		Adjunct	ISE 6425
Pizor	Chris	MS	Cybersecurity	Certified Instructor		Adjunct	ISE 5201
Rios	Billy	MS	Information Systems	Certified Instructor		Adjunct	ISE 6515
Shewmaker	James	BS	Computer Science	Certified Instructor		Adjunct	ISE 6360
Siles	Raul	MS	Computer Science	Certified Instructor		Adjunct	ISE 6325
Soni	Anuj	MS	Information Systems Management	Certified Instructor		Adjunct	ISE 6460
Spitzner	Lance	MBA	Business	Certified Instructor		Adjunct	ISE 5300
Szczepankiewicz	Peter	MS	Information Technology Managem	Certified Instructor		Adjunct	ISE 6325, ISE 6445
Toussain	Matthew	MS	Information Security Engineering	Certified Instructor		Adjunct	ISE 6320
Valenzuela	Ismael	BS	Computer Science	Certified Instructor		Adjunct	ISE 6240
Williams	Donald	MS	Information Technology	Certified Instructor		Adjunct	ISE 5201, ISE 5401
Zimmerman	Eric	BS	Computer Science	Certified Instructor		Adjunct	ISE 6425