SANS Technology Institute

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

ED SKOUDIS
President

DAVID HOELZER
Dean of Faculty

JOHANNES ULLRICH, Ph.D.
Dean of Research

ERIC PATTERSON
Executive Director

BETSY MARCHANT
Assistant Director

October 21, 2022

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,

It is with great enthusiasm that the SANS Technology Institute submits the attached proposal to create a Lower Division Undergraduate Certificate in Cybersecurity Fundamentals.

We believe that this program will provide talented Maryland students with a powerful and effective introduction to the fundamental skills and knowledge needed to succeed in an associate's program, an upper division undergraduate certificate, or a bachelor's degree program in cybersecurity. We continue to observe that issues such as imposter syndrome, or even simply just doubt about one's suitability and potential for a comprehensive academic cybersecurity program, are limiting factors preventing more young people or career changers from exploring the possibility of a rewarding cybersecurity career. This program, the first of its kind in Maryland, seeks to lower those barriers to entry in an affordable fashion.

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.

Ed Skoudis
President
SANS Technology Institute

Office Use Only: PP#

MHEC
Creating a state of achievement

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

Institution Submitting Proposal	SANS Technology Institute

Each action below requires a separate proposal and cover sheet.

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

Department Proposing Program	SANS Technology Institute
Degree Level and Degree Type	Lower division undergraduate certificate
Title of Proposed Program	Cybersecurity Fundamentals (CSF)
Total Number of Credits	12
Suggested Codes	HEGIS: 5199 CIP: 11 1003
Program Modality	□ On-campus ☑ Distance Education (*fully online*) □ Both
Program Resources	☑ Using Existing Resources □ Requiring New Resources
Projected Implementation Date	□ Fall □ Spring ☑ Summer Year:2023
Provide Link to Most Recent Academic Catalog	URL: https://assets.contentstack.io/v3/assets/blt36c2e6352127
Preferred Contact for this Proposal	Name: Eric Patterson Title: Executive Director Phone: 440-321-3040 Email: epatterson@sans.edu
President/Chief Executive	Type Name: Signature: Date:13 OCT 2022
Approval/Endorsement by Governing Board	Type Name: Signature: Date:23 SEP 2022

Revised 5/7/18

PROPOSAL FOR A

LOWER DIVISION UNDERGRADUATE CERTIFICATE IN CYBERSECURITY FUNDAMENTALS

SANS Technology Institute

Table of Contents

A. Centrality to Institutional Mission Statement and Planning Priorities

1. Program Description

The SANS Technology Institute (STI) proposes to launch a Lower Division Undergraduate Certificate in Cybersecurity Fundamentals (CSF). CSF is designed to enable lower division students to be more properly and strongly prepared to confidently start and succeed at upper division cybersecurity studies, especially at the SANS Technology Institute but ostensibly at any academic institution in Maryland. This certificate will prepare students to more confidently enter into upper division cybersecurity studies by providing specifically designed classes to bridge the gap from basic computer science and information technology coursework into the more specialized study of cybersecurity topics. Under the CSF program, students will complete 12 credit hours of courses in which they will earn one professional cybersecurity certification relied upon by U.S. law enforcement, intelligence services, military organizations, large corporations, and contractors to validate the potential and competencies of their new-to-cyber workforce. CSF students will also develop and demonstrate proficiency in the fundamental technologies and skills of mathematics and Python coding that serve as the baseline for all professionals in cybersecurity. The CSF program was designed in partnership with some of our most senior and experienced faculty to provide this solid set of foundational skills for those who recognize that they need it, as well as to serve as a remedial pathway for those who apply to upper division undergraduate programs at STI but who might not have performed well enough on our proprietary aptitude assessments.

2. Relation to the Mission and Strategic Goals of the SANS Technology Institute

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

The first and most critical of STI's four strategic goals in its 2021–2026 Strategic Plan is to "dramatically increase the number of graduates prepared to enter the professional cybersecurity workforce and to lead cybersecurity teams, programs, and efforts." We have had stunning success in producing alumni of the graduate programs who are making a profound difference in the cybersecurity posture of the organizations where they work, and we have begun to produce an increasing number of highly skilled entry-level professionals by way of our relatively newer undergraduate programs.

However, STI is one of only a small number of institutions that is producing technical talent with deep hands-on mastery of cybersecurity, and all those institutions together are producing only a tiny fraction of the people with advanced technical hands-on skills that the nation needs. STI is particularly limited in our student numbers because many excellent candidates have not completed an undergraduate degree and are thus not eligible for our graduate programs, and/or are uncertain about their background skills and preparation to enter straight into a technically rigorous undergraduate cybersecurity program. We believe this new preparatory program will increase the number of individuals entering the cybersecurity workforce with deep, hands-on mastery of cybersecurity and will also increase, over time, the number of students able to complete the STI master's degree program and go on to become cybersecurity leaders.

3. Funding for the Program

STI's finances are sound. The school has adequate cash flow to fund the new program through to the time it breaks even, for five years if necessary. In addition, STI's parent organization, the SANS Institute, is willing and able to provide additional funds if needed.

4. STI's Commitment to the Long-Term Success of the Program

The CSF program will be critically valuable to STI in meeting its top strategic objective of increasing the number of new entry-level cybersecurity professionals. Thus, the program has and will continue to have the highest visibility and priority for STI's president, management, and administrative staff.

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

1a. Critical Need for the CSF Program

Maryland, like the rest of the nation, continues to lose ground in its efforts to close the cybersecurity skills gap. Despite the ongoing establishment of more and more undergraduate cybersecurity programs, the number of unfilled cybersecurity jobs continues to increase. Nationally, that number currently sits at more than 714,000 vacant job openings, against a total national cybersecurity workforce of approximately 1.1 million cybersecurity professionals.[1]

Put another way, even with all the ongoing effort, nearly 39% of cybersecurity jobs in this country remain unfilled. In 2016, US colleges and universities graduated only about 64,000 students with degrees in computer science or information technology.[2] Even if all those computer science and IT majors end up in cybersecurity, and they won't, it would take more than a decade to come close to closing the skills gap. Thus, we are realistically going to, as a nation, continue to lose ground in this fight to create more skilled cybersecurity professionals.

High school students largely continue to remain in the dark about the need for and potential in this critical, high demand, profession which provides stunningly high compensation even for brand new entry-level professionals. Almost unbelievably, currently only about 35% of high schools in this country teach some form of computer science.

Yet, our ongoing experience here at the SANS Technology Institute, where we utilize our proprietary, psychometrically based aptitude assessment test for both undergraduate and graduate applicants, shows that we are succeeding at taking complete newcomers to the field, even complete newcomers to technology, and helping them to succeed and to quickly find meaningful and highly compensated employment. Since the inception of our undergraduate programs just a few years ago, we have witnessed 93% of our undergraduate alumni finding their first cybersecurity job within 6 months of graduation. More than half of those students receive their first job offer while still in their program, prior to graduation, and the preponderance of the 7% who have not found that first job are typically still finishing their bachelor's degree elsewhere having already completed our undergraduate certificate program. Those successful student outcomes are bolstered by an average starting salary, since program inception, of $94,000 for these STI undergraduate students; more recently, for our undergraduate alumni within just the past six months, that average starting salary has actually increased to $104,000.

[1] Source, Cyberseek.org, https://www.cyberseek.org/heatmap.html.

[2] Cybersecurityventures.com, https://cybersecurityventures.com/only-3-percent-of-u-s-bachelors-degree-grads-have-cybersecurity-related-skills/.

Given these successes, the SANS Technology Institute feels that it can do more by widening the onramp for a greater number of what we might have considered, thus far, to be marginally inadmissible students. That is the aim of this proposed program in Cybersecurity Fundamentals.

1b. The Key Benefit of CSF

Our relatively newer undergraduate programs have witnessed amazing growth and equally amazing student outcomes. However, even with these successes we continue to encounter students who are either marginally unsuited for our undergraduate programs or who doubt their ability to succeed in those programs. Nearly always, this unpreparedness or doubt stems from a lack of prior study of and success in the fundamental STEM skills which are required to succeed in the field of cybersecurity.

CSF graduates will be eminently prepared to enter into and succeed in cybersecurity studies, whether at the SANS Technology Institute or at any other college or university in Maryland.

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

This section is presented using the Maryland State Plan for Postsecondary Education, 2017-2021, as it appears that the updated plan for 2022 – 2025 has not yet been published.

This proposed CSF program is ideally designed to support “Strategy 9: Strengthen and sustain development and collaboration in addressing teaching and learning challenges,” as well as the overall goal of “Student Success with Less Debt.”

As already touched upon above, the opportunities for rewarding and remunerating careers in cybersecurity is unparalleled in modern times. Our undergraduate programs are proving that, every week and month. However, we see an unacceptably large number of potential students who are, or simply feel, unprepared to take on the challenges of cybersecurity studies that lead to these amazing student outcomes. Rather than attempt to solve for the entirety of the problems of STEM education in this country, our expert faculty have winnowed down the foundational requirements of study to just the three courses described in this proposal.

Addressing this learning challenge, and allowing these otherwise excluded, or self-excluded, residents of Maryland to pursue an incredible opportunity in cybersecurity is the primary aim of the CSF program. In doing so via these three courses, we also aim to keep student debt to an absolute minimum as they pursue a career where starting salaries are commonly six figures.

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

1. Market Demand for Cybersecurity Professionals

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

CyberSeek states that the supply of cybersecurity workers nationally is “low,” with 714,548 job openings relative to a total employed workforce of 1,091,575 (a ratio of 0.65, or, for every 100 employed workers, the market seeks another 65 people). In Maryland alone, CyberSeek shows that there are 23,252 current job openings, with 6,617 such openings that specifically request GIAC certification holders, with a current

Maryland cybersecurity workforce of 46,023 a ratio of 0.51, or, for every 100 employed workers, the market seeks another 51 people). 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.

2. Demand for CSF Graduates

At a minimum, as an alternative pathway for marginal applicants to master the fundamental skills and to demonstrate their preparedness for our own undergraduate programs, we know that we have our own internal demand for graduates of the proposed CSF program. A review of our admissions data reveals that we would have likely offered this alternative matriculation pathway to at least 45 students just so far this year, and close to 60 students since we implemented our upper division undergraduate programs.

Externally, we believe that this program will be attractive to potential students at STI or elsewhere who are interested in the cybersecurity field but are hesitant to commit to a full and more expensive cybersecurity degree program without a better understanding of their aptitude, potential, and ability to learn and master the fundamental skills.

3. Current and Projected Supply of Cybersecurity Graduates

The Maryland Higher Education Trend Data and Program Inventory data[3] indicates that, in 2019, 24 campuses in Maryland graduated approximately 450 undergraduate students from some type of applied, technical cybersecurity degree or certificate program. This compares to the Cyberseek job data, above, where there are currently 23,252 cybersecurity job openings in Maryland.

That small number of new Maryland cybersecurity graduates in 2019 is clearly insufficient to meet the needs of the cybersecurity industry in Maryland, and we should be taking all steps possible to attract possible talent into the field. Here's how Ellen Nakashima describes the competition for cyber talent in an article in the *Washington Post*: "Along the Baltimore-Washington Parkway, the concentration of government agencies and contractors brimming with computer geeks rivals any cyber defense area on the planet." This booming Maryland industry is, one must thusly conclude, an area where employers are still required to hire talent from outside the state to fill their job roles.

D. Reasonableness of Program Duplication

1. Similarities and Differences between the CSF Program and Other Programs Awarding Lower Division Undergraduate Certificates in Cybersecurity

In determining whether a program is unreasonably duplicative, according to the Maryland Code of Regulations (COMAR 13B.02.03.09(C), the Secretary shall consider (a) the degree to be awarded; (b) the area of specialization; (c) the purpose or objectives of the program to be offered; (d) the specific academic content of the program; (e) evidence of equivalent competencies of the proposed program in comparison to existing programs; and (f) an analysis of the market demand for the program. The analysis on unreasonable duplication shall include an examination of factors including (a) the role and mission; (b) accessibility; (c) alternative means of educational delivery, including distance education; (d) analysis of enrollment characteristics; (e) residency requirements; (f) admissions requirements; and (g) educational justification for the dual operation of programs broadly similar to unique or high-demand programs at historically black institutions.

[3] https://data.mhec.state.md.us/mac_Trend.asp

Our analysis of these factors demonstrates that the STI CSF program is not unreasonably duplicative, and that it is an important addition to the educational offerings available to students in Maryland.

Of the 450 undergraduate cybersecurity students who graduated in 2019, about 100 of those did so by earning a lower-level undergraduate certificate. Three of those existing lower division certificate programs graduated zero students, and none graduated more than 30 students.

The STI CSF program will be unique among these offerings in that it is specifically designed not as a stand-alone program, but as a bridge to higher-level studies which result in a more skilled and more highly sought after entry-level professional. The CSF program will enable otherwise marginal students to confidently pursue the rigorous, advanced, and technical content available in an upper division undergraduate program, whether that be at STI or elsewhere, and to earn an industry recognized GIAC certification as part of their studies.

Specific Academic Content of the Program; Evidence of Equivalent Competencies

The CSF program, as a preparatory and remedial program, offers students program elements not currently available in any other approved lower-level undergraduate certificate programs:

1. *Focused fundamentals.* Other colleges in Maryland offer broad lower-division undergraduate certificate programs that introduce the student to basic cybersecurity concepts and skills. Our upper-division undergraduate certificate program and our bachelor's degree programs at the SANS Technology Institute are growing rapidly and already achieve this aim for our institution and for the state of Maryland. Rather, the CSF program will, instead, pointedly prepare uncertain or otherwise marginal students to be more fully and successfully prepared to engage with a more comprehensive upper-division program of study.
2. *Effective conceptual translation from information technology and computer science concepts to information security knowledge.* As a condensed, effective, and efficient way for students from non-technical or non-STEM backgrounds to pivot into cybersecurity, the CSF program will teach information technology concepts and principles not as a stand-alone subject, but very intentionally in a manner which will allow the student to then translate that knowledge into the security perspective.

Alternative Means of Educational Delivery, including Distance Education

The CSF program will be available as an entirely asynchronous and online program of study, allowing for working students and busy professionals to engage with the courses and content on a schedule that works for them individually.

2. Admissions Requirements

STI's admission requirements for the CSF program require a 2.5 GPA. For students who have applied to one of our upper-division undergraduate programs but who have been denied due to a low score on our proprietary aptitude assessment test, the CSF program will be an affordable and viable alternative pathway to demonstrating a satisfactory level of fundamental knowledge and academic grit that can allow them to successfully transition into a more challenging upper-division program of study.

E. Relevance to High-Demand Programs at Historically Black Institutions (HBIs)

Not applicable

F. Relevance to the Identity of Historically Black Institutions (HBIs)

Not applicable

G. Adequacy of Curriculum Design and Delivery to Related Learning Outcomes (COMAR 13B.02.03.10)

1. Describe how the proposed program was established, and also describe the faculty who will oversee the program.

CSF was established as a means of meeting STI's strategic goal of "materially increasing the number of technically skilled professionals and leaders who strengthen global information security through innovative and flexible approaches to learning." Our faculty and administrators recognized that students who have the interest in pursuing a career in cybersecurity often do not come from a traditional information technology, computer science, or STEM background, but that these same students often lack some of the fundamental skills needed for them to quickly succeed and feel confident in their ability to pursue advanced and rigorous cybersecurity studies.

Our Faculty Committee decided that these fundamental skills, once filtered down to the truly essential, consist of basic coding experience, solid mathematical ability, and a firm understanding of essential information technology concepts viewed through the lens of cybersecurity.

With that in mind, three of our leading faculty members stepped forward to design these courses.

Applied Mathematics for Information Security Professionals – David Hoelzer

Introductory Python – Mark Baggett

Foundations: Computers, Technology, & Security – James Lyne

<u>David Hoelzer</u>

David Hoelzer is our Dean of Faculty and is a SANS Fellow. 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. 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.

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. David is the course author and primary instructor for SECC 503, Intrusion Detection In-Depth, and for SEC595: Applied Data Science and Machine Learning for Cybersecurity Professionals.

David has written and contributed to more than 15 peer reviewed books, publications, and journal articles. He holds a BS in IT and an MS in Computer Science.

Mark Baggett

Mark is a SANS Senior Instructor and is the course author and primary instructor for SEC573: Automating Information Security with Python and for SEC673: Advanced Information Security Automation with Python.

Mark has a master's degree in information security engineering from the SANS Technology Institute and is the 15th person in the world to receive the prestigious GIAC Security Expert certification (GSE). He also holds GPYC, GXPN, GPEN, GCIA, GCIH, GSEC, GWAPT, and GCPM certifications.

An active participant in the information security community, Mark is the founding president of The Greater Augusta Information Systems Security Association (ISSA) chapter which has been extremely successful in bringing networking and educational opportunities to Augusta information technology workers. He's also co-founder of the BSidesAugusta Information Security Conference and has written a number of articles on information security topics.

James Lyne

James is a SANS Certified Instructor, as well as the founder of CyberStart, a gamified cyber security learning platform for young adults used by hundreds of thousands. James has given multiple TED talks, including at the main TED event. He's also appeared on a long list of national TV programs to educate the public including CNN, NBC, BBC News, Bill Maher and John Oliver. As a spokesperson for the industry, he is passionate about talent development, regularly participating in initiatives to identify and develop new talent for the industry. He is the course author and primary instructor for SEC 275: Foundations: Computers, Technology, & Security.

2. Describe educational objectives and learning outcomes appropriate to the rigor, breadth, and (modality) of the program.

a) The CSF program is designed to provide an accelerated path to identify and prepare more talented potential for a career in cybersecurity. The program will achieve that aim by way of the following objectives and outcomes:

- Distill some of the most important mathematics foundations that apply to computer science and information security
- Learn basic Python coding skills in Windows and Linux environments.
- Obtain a level of sufficient theoretical understanding and applied practical skills that will enable the student to speak the same language as industry professionals.

To meet those objectives the CSF program will enable students to achieve the following learning outcomes:

- Demonstrate an understanding of the mathematics that underpin digital information systems so that students can reason on and apply mathematics as they interface with computer science and cybersecurity topics and systems. Discrete topics covered will include:
  - Algebra
  - Definitions of functions (even, odd, continuous, discontinuous)
  - Manipulation of first and second order equations
  - Solving for roots of second order equations

  - Probability
  - Boolean Algebra / set operations
  - Binary and other number systems
  - Statistics
  - Mean, median, mode, and statistically robust variations
  - Variance measures and their statistically robust variations
  - Sampling
  - Approaches to inference
  - Calculus Foundations I
  - Continuous vs discontinuous functions
  - The fundamental theorem of calculus
  - Limits
  - Euler's constant
  - Calculating derivatives
  - Automatic differentiation
  - Calculus Foundations II
  - Definite integrals
  - Indefinite integrals
  - Sequences
  - Series
  - Signals analysis applications
  - Partial differentials
  - Linear Algebra
  - Solving systems of equations
  - Transformation of basis vectors
  - Linear transformations
  - Affine transformations
  - Transformation matrices
  - Quaternions
  - Eigenvalues and Eigenvectors
  - Principal component analysis
  - Linear Discriminant Analysis

- Install and maintain Python programs and modules
- Demonstrate basic Python programming concepts
- Understand Python functions, IDEs, modules, and lists
- Understand and be able to execute basic file IO
- Develop fundamental skills and knowledge in key IT subject areas to include:

  - Computer components & concepts
  - Operating systems, containers, & virtualization
  - Linux
  - Networking fundamentals
  - Search engine & servers
  - Windows foundations
  - Advanced computer hardware (CPU & memory)

- Encryption
- Introduction to basic security concepts
- Introduction to forensics
- Introduction to reconnaissance, exploitation, and privilege escalation
- Introduction to network & computer infiltration (lateral movement)

3. Explain how the institution will:
a) provide for assessment of student achievement of learning outcomes in the program
b) document student achievement of learning outcomes in the program

For the CSF program, STI will measure student achievement of learning outcomes using two different methods. In the mathematics course and the Python coding course, students will be assessed via a series of practical, problem-solving challenges culminating in an online final exam.

In the security foundations course, students will be required to sit for the Global Information Assurance Certification (GIAC) GFACT examination (https://www.giac.org/certifications/foundational-cybersecurity-technologies-gfact/).

4. Provide a list of courses with title, semester credit hours and course descriptions, along with a description of program requirements

CSF Course Name	Number	Credit hours
Applied Mathematics for Information Security Professionals	CSF 2395	3
Introductory Python	CSF 2473	3
Foundations: Computers, Technology, & Security	CSF 2275	6
	Total	12

Course Descriptions:

CSF 2395: Applied Mathematics for Information Security Professionals

This course will cover the most important mathematics foundations that apply to computer science and information security, namely the fundamentals of cryptography and the notions of sets and closed systems. At the conclusion of this course, students will be able to reason on and apply fundamental mathematics as they interface with computer science and cybersecurity topics.

CSF 2473: Introductory Python

This hands-on course will teach students by having them actively write Python code so that they can see successful results and learn by doing. Using that practical approach, this course will teach students how to install and maintain Python programs and modules, utilize basic Python programming concepts such as functions, IDEs, modules, lists, and basic file input / output.

CSF 2275: Foundations: Computers, Technology, & Security

The course provides students with the practical learning and key skills to empower future cybersecurity learning. Students will be able to progress from zero technical and security knowledge to a level of sufficient theoretical understanding and applied practical skills that will enable them to speak the same language as industry professionals by developing fundamental skills and knowledge in key IT subject areas, as discussed above in the section on learning outcomes.

5. Discuss how general education requirements will be met, if applicable.

Not applicable.

6. Identify any specialized accreditation or graduate certification requirements for this program and its students.

Not applicable.

7. If contracting with another institution or non-collegiate organization, provide a copy of the written contract.

Under a formal Memorandum of Understanding (MOU), STI outsources to SANS (STI's parent organization) many of the operational and administrative functions required to support operations, including establishment of most of our learning environments (physical and virtual), financial transactions, accounting, technology, and other administrative support services. Using this mechanism, STI benefits from SANS's economies of scale and transforms typically high-fixed-cost elements into manageable, smaller variable costs. STI also benefits from its relationship with Global Information Assurance Certification (GIAC), a sister company also owned by SANS. GIAC was established in 1999 to develop and offer exams and certifications that validate whether an individual has gained sufficient competency or mastery of the complex topics taught in SANS courses, and most technical STI courses require students to pass a GIAC certification exam. GIAC exams are the product of broad-based job task analyses that incorporate feedback from hundreds of industry participants. Exam questions and answers and scoring patterns are reviewed and assessed by a PhD in psychometrics. Many of these certification exams have been designed with such a degree of quality that they are, themselves, certified by the American National Standards Institute (ANSI). Thus, learning in STI's CSF courses is validated not by exams created by individual faculty members, but by assessments created by a highly specialized exam creation and testing organization that also keeps these exams current with changing professional requirements over time.

The MOU has enabled all STI degree programs since STI was established and was most recently reviewed and approved during a Middle States accreditation team visit.

A more complete description of the corporate entities, along with the MOUs, is provided in Appendix 1.

8. Provide assurance and any appropriate evidence that the proposed program will provide students with clear, complete, and timely information on the program.

STI has a demonstrated record of completeness and transparency in all its academic programs and commits to maintaining a very high level of clarity, thoroughness, 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. You can see evidence of the clarity and completeness of STI's existing undergraduate programs at
Undergraduate admissions: https://www.sans.edu/admissions/undergraduate/?msc=main-nav,
Bachelor's degree academic page: https://www.sans.edu/cyber-security-programs/bachelors-degree/?msc=main-nav, and
Undergraduate certificate academic page: https://www.sans.edu/cyber-security-programs/undergraduate-certificate/?msc=main-nav.

9. Provide assurance and any appropriate evidence that advertising, recruiting, and admissions materials will clearly and accurately represent the proposed program and the services available.
We commit to provide only clear and accurate information in our advertising, recruiting, and admissions material. Evidence of the clarity of our advertising and recruiting and admissions information for undergraduate studies may be found at:
https://www.sans.edu/admissions/undergraduate/?msc=main-nav

H. Adequacy of Articulation

Not applicable.

I. Adequacy of Faculty Resources (outlined in COMAR 13B.02.03.11).

The members of the CSF faculty are widely respected scholar-practitioners. The faculty serving the students of the proposed CSF program is comprised of the same instructors who currently teach the 1,000 enrolled graduate students and the 400 enrolled undergraduate students enrolled at STI. We believe that our faculty is adequate in both capability and number to serve this new program.

The following is a list of faculty members with credentials and courses taught:

Name	Degree	Field of Degree	Academic Title / Rank	Status	Course(s)
David Hoelzer	MS	Computer Science	Dean and Faculty Fellow	Full-time	CSF 201
Mark Baggett	MS	Information Security Engineering	Senior Instructor	Full-time	CSF 202
James Lyne	MS	Information Security	Certified Instructor	Full-time	CSF 203

J. Adequacy of Library Resources (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, which 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.

K. Adequacy of Physical Facilities, Infrastructure, and Instructional Equipment

This program will be offered online only, using the well-established OnDemand platform that STI has had since years before COVID and the rest of academia needing to shift to online teaching.

This OnDemand delivery systems currently serve more than 35,000 students each year and has significant capacity for growth. In evidence provided to Middle States Commission on Higher Education for STI's accreditation review, GIAC test results for students who studied using the online modalities were as high as those who studied at the residential institutes. Thus, the instructional infrastructure is capable of supporting hundreds of CSF students with no additional resources or strain upon the platform.

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

1. Complete Table 1: Resources and Table 2: Expenditures . Finance data for the first five years of program implementation are to be entered.
2. Provide a narrative rationale for each of the resource categories.

Table 1: RESOURCES

Resource Categories	Year 1	Year 2	Year 3	Year 4	Year 5
1. Reallocated Funds	0	0	0	0	0
2. Tuition/Fee Revenue (c + g below)	$154,500	$257,500	$386,250	$515,000	$515,000
a. Number of F/T Students	60	100	150	200	200
b. Annual Tuition/Fee Rate	$2,575	$2,575	$2,575	$2,575	$2,575
c. Total F/T Revenue (a x b)	$154,500	$257,500	$386,250	$515,000	$515,000
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	0	0	0	0	0
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)	$154,500	$257,500	$386,250	$515,000	$515,000

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 Year 1 assumes the CSF program admits 60 full-time students who each pay $2,575. We believe this is an appropriate estimate given our analysis of our admissions data for our upper-division undergraduate programs.

In each subsequent year, we project that enrollment will progress to 100, then 150, and finally to 200 students completing the CSF program in each of Years 2 – 5, with no planned tuition increases. We believe expectations for significant growth are reasonable, and are likely conservative.

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

Expenditure Categories	Year 1	Year 2	Year 3	Year 4	Year 5
1. Faculty (b + c below)	$23,500	$39,000	$58,500	$78,000	$78,000
a. # Sections offered	N/A	N/A	N/A	N/A	N/A
b. Total Salary	$18,000	$30,000	$45,000	$60,000	$60,000
c. Total Benefits	$5,500	$9,000	$13,500	$18,000	$18,000
2. Admin. Staff (b + c below)	$25,740	$39,000	$58,500	$78,000	$78,000
a. # FTE	.33	.5	.75	1	1
b. Total Salary	$19,800	$30,000	$45,000	$60,000	$60,000
c. Total Benefits	$5,940	$9,000	$13,500	$18,000	$18,000
3. Support Staff (b + c below)	0	0	0	0	0
a. # FTE	0	0	0	0	0
b. Total Salary	0	0	0	0	0
c. Total Benefits	0	0	0	0	0
4. Equipment	0	0	0	0	0
5. Library	0	0	0	0	0
6. New or Renovated Space	0	0	0	0	0
7. Other Expenses	$0	$0	$0	$0	$0
TOTAL (Add 1 – 7)	$49,240	$78,000	$117,000	$156,000	$156,000

Faculty

The CSF program will be delivered solely via our online, asynchronous OnDemand modality. Our students engage with the recorded coursework at their own pace and on their individualized academic plan, leading to us not offering traditional sections.

Thus, our faculty for this program are paid a stipend for each registration, with their actual work consisting of the upfront creation of the course and the occasional subsequent review and revision of the content.

While the costs associated with the faculty who teach these students is embedded in the payments associated with the Memorandum of Understanding between STI and SANS, we have separated out projected amounts for Faculty Salary and Faculty Benefits in Table 2.

Administrative and Support Staff

The STI undergraduate programs currently operate at a ratio of students to administrative staff ratio of 150:1 (including both full-time administrative and support staff). A pending reorganization will allow us to increase this ratio to 200:1 without any dilution of student support and outcomes. Average salary and benefit information is reflective of our current cost experience and market expectations.

Equipment, Library, and New and/or Renovated Space

The CSF 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

As described elsewhere, a core design element of the SANS Technology Institute is 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 CSF program will also benefit from this financial arrangement. 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.

M. Adequacy of Provisions for Evaluation of the Program (outlined in COMAR 13B.02.03.15).

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

1. *Every day, in every STI class, every student is expected to complete an evaluation of the teaching effectiveness, currency, and value of the course material, and the quality of the labs, exercises, and other aspects of their learning experience.* Their forms are processed by an evaluation team and results are delivered by 11:30 that evening to STI's president and senior staff. The evaluation team follows up on all strong concerns and, in cases in the past when a faculty member was clearly struggling, has replaced the teacher by noon the next day based on the evaluations. In addition, the evaluation team compiles and feeds course content suggestions or concerns to the course author for consideration or inclusion in the annual (or sometimes more frequent) course updates. Data on labs or other technology go to the appropriate teams for continuous or major product improvement. This evaluation system is also used in vLive and Simulcast distributed learning modalities. For On-Demand, the evaluation cycle is based on module completion rather than days, but the system functions identically and in fact responses are easier to process because entries are already in digital form when submitted.

2. *Evaluation of course-level student outcomes uses reliable measures of mastery, not subject to variability, that are associated with individual faculty members' understanding of the course outcomes.* Each course has an associated examination that is recognized as a widely accepted and valued way to validate mastery of the course outcomes. For example, all CSF students will be required to complete a course in which they learn incident handling techniques, common attack techniques, and the most effective methods to stop intruders using those attack techniques. The exam and certification associated with this course is called the Global Cybersecurity Incident Handler (GCIH) test and certification. The value of this exam is demonstrated by the fact that each year employers pay for more than 9,000 of their employees and job candidates to take this course and sit for the GCIH exam (pass rate of approximately 79%). The acceptance of the exam is validated by the U.S. Department of Defense (DoD) directive that names GCIH certification as proof that a DoD employee or contractor is capable of taking on the highest of three levels of technical cybersecurity roles in DoD. The GIAC certifications used for evaluating student mastery of course objectives are updated using a large-scale job-task analysis that interviews practitioners at least every three years. This process, along with the psychometric assessments that shape question assessment, is subject to regular review by the American National Standards Institute. GIAC exams increasingly include hands-on test questions where students can demonstrate they can use what they learned.

N. Consistency with the State's Minority Student Achievement Goals (outlined in COMAR 13B.02.03.05 and in the State Plan for Postsecondary Education).

Strategy 4 of the Maryland State Plan calls for collaboration between historically black universities and colleges (HBUCs) and other institutions to ensure equal educational opportunity for all Marylanders. To identify students who will excel in the CSF program, SANS will use the CyberStart talent identification simulator that allows people who have never worked in IT to discover whether they would be good at cybersecurity and like it. We will use the simulator in all Maryland community colleges that choose to participate and also make the same gamified simulation available to students in HBCUs that choose to be partners, and we will follow up with additional support for the HBCUs to help their talented students pursue further study in cybersecurity and its foundations. The simulator and evidence of its reliability are further described in Section B.2 above, **Alignment with the 2017–2021 Maryland State Plan for Postsecondary Education.**

O. Relationship to Low-productivity Programs Identified by the Commission

N/A

P. If Proposing a Distance Education Program, Please Provide Evidence of the Principles of Good Practice (outlined in COMAR 13B.02.03.22C).

See Appendix 2 for the evidence that this program complies with the Principles of Good Practice.

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 consistentinterpretation 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:

Eric A. Patterson
Executive Director
SANS Technology Institute

____
Date:

Agreed to on behalf of SANS:

Peggy Logue
Chief Financial Officer
SANS Institute

____
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
RES5900	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.

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

Table A4.1. 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 Bachelor of Professional Studies in Applied Cybersecurity program have been validated by the faculty as appropriately rigorous and broad and are integrated into each course and measured quantitatively through ANSI-standardized certification exams for the three advanced courses and through integrated testing in each of the other courses.

(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 has been assessed and approved by STI faculty. But that is not the end of the development process. The distance learning technology is continuously assessed 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 running the Elluminate platform, running labs, and assisting with student questions. Many instructors prefer that the moderator relay questions from the virtual students by raising his or her hand and reading the question.

Audio Tips

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

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

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

Starting Class

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

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

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

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

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

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

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

Teaching Tips

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

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

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

19. All scripts, videos, demos, etc. that you wish to show to students must be shared with GoToTraining's application sharing feature.
20. Remote students' systems (and your host's network) can be slowed down if you send very large files. If a file is necessary for class try to send it before class or during a break. If it is not course-related (e.g., music while on break), consider not sending it.
21. Use the GoToTraining timer when breaking from lecture so remote students know when class will be resuming; tell the moderator how many minutes you would like and they will set up the timer for you.
22. When breaking for lunch, please explain to students that they will need to log out of the morning session and log into the afternoon session upon their return.
23. Allow plenty of time to log into GoToTraining when arriving in the morning or returning from lunch. Depending on the location, you may have to extend the lunch break.
24. Conduct a quick audio check after each break and lunch to confirm that your microphone is on and that your remote students can hear you.

Suggested Best Practices

Jason Fossen (SANS Senior Instructor):

- o 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.
- o 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.
- o Return early after lunch to log back into GoToTraining.
- o Make sure your Internet connection is wired and not shared by the students.
- o Make sure to have the vLive emergency contact info on hand.
- o 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 (SANS Senior Instructor):

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

(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, on the SANS.EDU website at https://www.sans.edu/academics/

- Course and degree requirements are posted online in the STI Course Catalog at https://www.sans.edu/downloads/STI-Course-Catalog-2018.pdf

- The nature of faculty/student interaction is described on our website at https://www.sans.edu/academics/course-delivery/more

- Assumptions about technology competence and skills are posted on our Admissions website at https://www.sans.edu/admissions/masters-programs

- Technical equipment requirements are posted with individual courses on the SANS course website. For example, for ACS 3504: 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 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 A4.2).

Table A4.2. 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 CSF students will be lower division students, likely at least 19 years old, and sufficiently well versed in information technology to have scored sufficiently high on the cyber aptitude test and simulator gain acceptance. 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 CSF students are currently being drafted. 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 implement the new CSF program. Further, because the undergraduate program is core to our mission and was specifically discussed during the Middle States 2018 Team Visit as a critical step for meeting that mission, we have demonstrated both the commitment and resources to maintain the program for many years.

(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." The assessment system and processes are detailed in Section M. This same system will be used in the distance learning component of the proposed CSF 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 CSF program will be measured by grades on the internationally standardized GIAC exams for each area of security. We compare these scores in distance and in-person learning modalities. As shown in Table A4.3, the GIAC test scores in distance learning are essentially identical to scores of students who used live, in-person residential training programs:

Table A4.3. Comparison of GIAC Exam Score Performance via Live and OnDemand Modalities, 2014–2017

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

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