SANS Technology Institute

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

September 15, 2024

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

Dear Dr. Rai,

I am pleased to submit, on behalf of the SANS Technology Institute, the attached proposal for substantial modification to our existing Bachelor of Science (B.S.) in Applied Cybersecurity program.

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#

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

Payment Submitted:	☑ Yes ☐ No	Payment Type:	☐ R*STARS #0000190603 ☉ Check # 0000190603	Payment Amount:	$250	Date Submitted:	9/9/2024

Department Proposing Program	Operations	
Degree Level and Degree Type	Undergraduate, Bachelor of Science	
Title of Proposed Program	Bachelor of Science (B.S.) in Applied Cybersecurity	
Total Number of Credits	120	
Suggested Codes	HEGIS: 0702.01	CIP: 11.1003
Program Modality	☐ On-campus ☐ Distance Education (fully online) ☑ Both	
Program Resources	☑ Using Existing Resources ☐ Requiring New Resources	
Projected Implementation Date (must be 60 days from proposal submisison as per COMAR 13B.02.03.03)	☐ Fall ☑ Spring ☐ Summer	Year:2025
Provide Link to Most Recent Academic Catalog	URL: https://sans.edu/media/Undergraduate-Course-Catalog.pd	
Preferred Contact for this Proposal	Name: Eva Dring	
	Title: Director of Academic Affairs	
	Phone: (301) 371-2142	
	Email: edring@sans.edu	
President/Chief Executive	Type Name: Ed Skoudis	
	Signature: Edward F. Skoudis	Date:9/15/2024
	Date of Approval/Endorsement by Governing Board:	06/28/2024

Revised 1/2021

Proposal for a Substantial Modification to an Existing Degree Program:

Bachelor of Science (B.S.) in Applied Cybersecurity

SANS Technology Institute

September 15, 2024

Table of Contents

TABLE OF CONTENTS **2**

A. CENTRALITY TO INSTITUTIONAL MISSION AND PLANNING PRIORITIES **4**

1. Program Description 4
2. Relation to Mission, Vision, and Strategic Goals of STI 7
3. Funding for the Program 9
4. Commitment to the Long-Term Success of the Program 9

B. REGIONAL OR STATEWIDE NEED AS IDENTIFIED IN THE STATE PLAN **9**

1. Demand and Need for Program 9
2. Alignment with Maryland State Plan for Postsecondary Education 10

C. MARKET SUPPLY AND DEMAND IN THE REGION AND STATE **11**

1. Industry, Employment Opportunities, and Expected Level of Entry 11
2. Market Demand 12
3. Anticipated Vacancies 12
4. Current and Projected Supply of Prospective Graduates 13

D. REASONABLENESS OF PROGRAM DUPLICATION **13**

E. RELEVANCE TO HIGH-DEMAND PROGRAMS AT HISTORICALLY BLACK INSTITUTIONS (HBIS) **16**

F. RELEVANCE TO THE IDENTITY OF HISTORICALLY BLACK INSTITUTIONS (HBIS) **17**

G. ADEQUACY OF CURRICULUM DESIGN, PROGRAM MODALITY, AND RELATED LEARNING OUTCOMES **18**

1. Establishment of Program and Faculty 18
2. Educational Objectives and Intended Student Learning Outcomes 19
3. Assessment and Achievement of Learning Outcomes 20
4. Course Requirements and Descriptions 21
5. General Education Requirements 25
6. Specialized Accreditation/Certification Requirements 25
7. Contract with Another Institution or Non-Collegiate Organization 26
8. Enrolled Student Communications 26
9. Prospective Student Communications 26

H. ADEQUACY OF ARTICULATION 26
I. ADEQUACY OF FACULTY RESOURCES 27
1. PROGRAM FACULTY 27
2. FACULTY RECRUITMENT AND DEVELOPMENT 29
J. ADEQUACY OF LIBRARY RESOURCES 32
K. ADEQUACY OF PHYSICAL FACILITIES, INFRASTRUCTURE AND INSTRUCTIONAL EQUIPMENT 34
L. ADEQUACY OF FINANCIAL RESOURCES WITH DOCUMENTATION 34
1. TABLE 1: PROGRAM RESOURCES 34
2. TABLE 2: EXPENDITURES 35
M. FINANCIAL DATA NARRATIVE 35
N. ADEQUACY OF PROVISIONS FOR EVALUATION OF PROGRAM 37
O. CONSISTENCY WITH THE STATE'S MINORITY STUDENT ACHIEVEMENT GOALS 38
P. RELATIONSHIP TO LOW PRODUCTIVITY PROGRAMS IDENTIFIED BY THE COMMISSION 38
Q. ADEQUACY OF DISTANCE EDUCATION PROGRAMS 38
1. ELIGIBILITY TO PROVIDE DISTANCE EDUCATION 38
R. COMPLIANCE WITH C-RAC GUIDELINES 38
APPENDIX I. CONTRACTS WITH RELATED ENTITIES 47
APPENDIX II: TECHNICAL ELECTIVE COURSE OPTIONS 57

A. Centrality to Institutional Mission and Planning Priorities

1. Program Description

The SANS Technology Institute proposes to substantially modify an existing degree program; the Bachelor of Science (B.S.) in Applied Cybersecurity. Established and approved by MHEC in 2021, the B.S. in Applied Cybersecurity is designed to provide a pathway for individuals who can demonstrate a high aptitude for cybersecurity-related work to earn a bachelor's degree and enter the workforce.

To graduate from the Bachelor's Degree in Applied Cybersecurity (BACS) program, students require a total of 120 credit hours: 50 credit hours from the SANS Technology Institute (SANS.edu) and 70 credit hours transferred from a community or 4-year college. Following the proposed modification, the 50 credit hours from SANS.edu will comprise eight required courses (previously seven), three elective courses, two experiential learning practicums, and a field experience practicum requirement.

The proposed modifications to the Bachelor's program will use existing institutional resources, and the changes will not require additional resources to implement.

Summary of Key Changed Elements

This proposal of substantial modification is the result of a comprehensive program review of the Bachelor's degree in 2024, which assessed (1) the content, balance, coherence, and rigor of the BACS curriculum, (2) the alignment of student performance and outcomes with the program's learning objectives and with the STI mission, and (3) the alignment of the program's learning outcomes with employers' needs and expectations.

The review team concluded that the BACS program is in a very good place overall, particularly in terms of enrollment levels, employability, meeting its goals, and quality of training. The proposed changes to the program are intended to:

1. Incorporate additional fundamental skills and knowledge areas into the core curriculum
2. Increase employability and career readiness of program graduates, by increasing opportunities to gain demonstrable hands-on cybersecurity experience through real-world challenges and a wider range of professional settings
3. More accurately distribute credit hours across the program curriculum, in line with the college's Credit Hour Policy
4. Provide a better supported and more coherent student experience as they move through the program's components
5. Increase scalability of the program.

Current Graduation Requirements

(with planned changes outlined in the final column)

Required Course	Course Name	Credits	Proposed Changes
BACS 3275	Foundations: Computers, Technology & Security	6	
BACS 3301	Introduction to Cybersecurity	4	This course will be removed from the program, due to overlap of content in the early core curriculum
BACS 3402	Effective Cyber Writing and Speaking	3	Credit hour value will be reduced from 3 to 2, and the course order will change
BACS 3401	Security Essentials	6	Credit hour value will be reduced from 6 to 4, and the course order will change
BACS 3504	Security Incident Handling and Hacker Exploits	4	
BACS 4503	Intrusion Detection in-Depth	6	Credit hour value will be reduced from 6 to 4, course order will change, updating course code to BACS 3503
BACS 3573	Automating Information Security with Python	4	This course will be preceded by an introductory level Python course
BACS 4999	Elective Course*	3	
BACS 4999	Elective Course*	3	
BACS 4999	Elective Course*	3	
BACS 4499	Internship	6	The single internship offering will be replaced by a 4-credit "Field Experience Practicum" requirement, within which students can choose between completing an internal work placement with the college, or an approved external professional placement

**Students choose electives from an approved list of courses. Electives can be taken within one specialist area, or chosen from across the full range. Please see list of acceptable technical elective courses and their full descriptions in Appendix II.*

Proposed Graduation Requirements

Required Course	Course Name	Credits	Changes from Existing Curriculum
BLOCK 1 *(courses must be taken in the specified order)*		**26**	2-block structure implemented, to aid coherence of student experience
BACS 3275	Foundations: Computers, Technology & Security	6	
BACS 3401	Security Essentials	4	Credit hour reduction and placement change
BACS 3504	Security Incident Handling and Hacker Exploits	4	Placement change
BACS 3402	Effective Cyber Writing and Speaking	2	Credit hour reduction and placement change
BACS 3373	Introductory Python	3	New program requirement
BACS 3573	Automating Information Security with Python	4	Placement change
BACS 3001	**Portfolio Practicum:** Experiential Learning through Cyber Challenges (Foundational) *To be completed at any time during Block 1 – can coincide with other courses.*	3	New program requirement – to increase portfolio-building opportunities, and to promote team-building and professional networking in a largely asynchronous program
BLOCK 2 *(courses can be taken in any order)*		**24**	2-block structure implemented, to aid coherence of student experience
BACS 4499 / BACS 4001	**Field Experience Practicum (choose one option):** Internal Internship/Work Placement (e.g. Apprentice Handler for SANS Internet Storm Center) External Internship (self-sourced professional placement, to be approved by the college) *To be completed at any time during Block 2 – can coincide with other courses*	4	Credit hour decrease, and additional external field experience option available

BACS 3500	Windows Forensic Analysis	4	Course added to core curriculum and course code updated – previously listed as an elective option ACS 4500
BACS 3503	Intrusion Detection in-Depth	4	Credit hour reduction, placement change, updated course code from BACS 4503
BACS 4999	Elective Course*	3	
BACS 4999	Elective Course*	3	
BACS 4999	Elective Course*	3	
BACS 3002	**Portfolio Practicum:** Experiential Learning through Cyber Challenges (Advanced) *To be completed at any time during Block 2 – can coincide with other courses.*	3	New program requirement – to increase portfolio-building opportunities, and to promote team-building and professional networking in a largely asynchronous program

**Students choose electives from an approved list of courses. Electives can be taken within one specialist area, or chosen from across the full range. Please see list of acceptable technical elective courses and their full descriptions in Appendix II.*

2. Relation to Mission, Vision, and Strategic Goals of STI

Mission and Vision

The BACS program continues to directly align with the formal mission of the SANS Technology Institute:

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

The program also continues to support the college's formal vision:

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

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

The Bachelor's degree program (BACS) advances this mission and vision by focusing on educating BACS students to work towards two outcomes: (1) proficiency in the fundamental technical knowledge and skills that serve as the baseline for all professionals in cybersecurity, and (2) early specialization in advanced skills that can be applied to particular areas of information security practice.

Strategic Goals

The BACS program not only aligns with STI's mission and vision, but is core to accomplishing the mission and key strategic goals. STI updated the institutional strategic plan in 2021, focusing on the next 5 years, which we believe are critical for the continuing success of the institution. As a result the following strategic goals were established:

(1) Continued Growth – Dramatically increase the number of graduates prepared to enter the professional cybersecurity workforce and to lead cybersecurity teams, programs, and efforts.
(2) Name Recognition – Significantly improve brand awareness, inside and outside of the cybersecurity community.
(3) Student Success – Continue to improve our retention rates, student experiences, and alumni outcomes.
(4) Industry Impact – Achieve, in measurable and impactful ways, the mission of our college to fill the critical skills and personnel gaps in the cybersecurity industry.

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 success in producing graduates of the Master's program who are making a profound difference in the cybersecurity posture of the organizations where they work, as documented in our Middle States Self-Study Report prepared for the most recent Team Visit Report to the Middle States Commission on Higher Education, and further recognized in the visiting team chair's report on that visit.

STI is one of only a small number of higher education institutions that is producing technical talent with deep hands-on mastery of cybersecurity, and all of those institutions together are producing only a tiny fraction of the people with advanced technical hands-on skills that the nation needs. Before the development of the Bachelor's degree, STI was previously particularly limited in our student numbers for graduate-level programs because many excellent candidates had not completed an undergraduate degree and were thus not eligible for our Master's degree. The Bachelor's degree has increased the number of individuals entering the cybersecurity workforce with deep, hands-on mastery of cybersecurity and has also begun to increase the number of students able to complete the STI Master's degree program and go on to become cybersecurity leaders.

The proposed modifications to the BACS curriculum, as outlined above, are specifically designed to support the third strategic goal of "Student Success", with specific proposed modifications to address retention rates, student experience and alumni outcomes.

The BACS curriculum is a driving factor in recruiting, educating and graduating information security professionals with a strong technical knowledge and skill set, therefore, the success of the program is critical to the success of the institute and its industry impact, as outlined in STI's fourth strategic goal.

3. Funding for the Program

STI's finances are sound. The school has had adequate cash flow to fund the new program through its early stages until the point of breaking even, for five years if necessary. Student fee income for this program now more than covers the costs of delivery (as outlined in section L). In addition, STI's parent organization, the SANS Institute, is willing and able to provide additional funds if needed.

4. Commitment to the Long-Term Success of the Program

The BACS program remains critically valuable to STI in meeting its top strategic objective. Thus, the program has, and will continue to have, the highest visibility and priority for STI's president and administrative staff. Most BACS courses are central elements of the SANS Institute's catalog of professional development educational offerings, so students can count on those courses to be continually available and frequently updated for a sufficient time that students who enroll will be able to complete the program.

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

1. Demand and Need for Program

Advancement and Evolution of Knowledge

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

Cyberseek, a website created by the National Institute of Standards and Technology (NIST), indicates that there were 469,930 cybersecurity job openings nationally from May 2023 through April 2024[i]. CyberSeek states that the supply of cybersecurity workers nationally is "very low" relative to the demand. In Maryland alone, CyberSeek shows that there are 27,730 job openings and 3,984 of those openings that specifically request GIAC certifications, which are obtained as a degree requirement of the BACS program. These data indicate a high demand not just for cybersecurity workers, but especially for those who have proven, by holding GIAC certifications, that they have the skills to do the job.

Societal Needs

Cybersecurity jobs are already an important part of Maryland's economy, with the state ranking in the top 10 nationwide for net tech employment; employer job postings for tech openings; and tech's economic impact as a percentage of state economy[ii]. With the increasing recognition of the vulnerability of critical public and private networks and the need to better protect those networks against constantly evolving threats, it is reasonable to expect that, in conjunction with the State Plan, Maryland will continue to attract additional information security workers and separating military veterans who wish to enter into this challenging field. This growth will call for educated technical professionals from a diverse range of backgrounds with a mastery of foundational cybersecurity technologies, competence in security tools and techniques, and knowledge of cyber hygiene and framework implementation, in addition to effective communication and reporting skills, and a strong professional network.

Relevance to Historically Black Institutions

Enabling HBIs to become equal partners with STI in overcoming the historical racial imbalance in cybersecurity in the United States can add an important strength to the identity of HBIs. The Bachelor's degree is essential to enabling STI to make its undergraduate academic programs available to students in HBIs. STI welcomes and supports applications from students from HBIs who meet the credit requirements – interested students are invited to take the Cyber Aptitude Test to see whether they are likely to excel in the STI Bachelor's program. Those who score well will be invited to include STI courses and the corresponding certifications in their undergraduate experience, in cooperation with their current institution.

2. Alignment with Maryland State Plan for Postsecondary Education

Student Access: Ensure equitable access to affordable and high-quality postsecondary education for all Maryland residents.

This program will continue to address the State Plan's goals to ensure equitable access to affordable and high-quality postsecondary education. Approximately 5% of current Bachelor's students fully fund their studies by way of employer tuition reimbursement, while another 60% utilize veteran education benefits, with nearly all of them using some combination of GI Bill benefits and employer tuition reimbursement to increase their knowledge and skills as they enter or further establish themselves in the civilian workforce. The college also offers its own range of financial assistance programs to reduce financial barriers to participation in our programs.

Student Success: Promote and implement practices and policies that will ensure student success.

STI's regular formal program review process that has led to the submission of this proposal for substantial modification to the BACS program is specifically designed to ensure student success. Program review teams are comprised of industry experts, program alumni, teaching faculty and college administrators, who bring together a combination of professional experience, personal experience, program performance data, student survey data, and a strong drive to innovate and stay ahead of the curve.

The BACS program makes substantial contributions to Maryland's goals by seeking to increase the number and quality of graduates who are desperately in demand in business and industry verticals across the state. To date, over 80% of BACS graduates have gained employment in either cybersecurity or a related IT field, with average graduate starting salaries exceeding $100,000 for the first time in 2024. Cybersecurity jobs are already an important part of Maryland's economy, with the state ranking in the top 10 nationwide for net tech employment; employer job postings for tech openings; and tech's economic impact as a percentage of state economy. Yet, even with this standing, the demand for skilled and educated cybersecurity practitioners is outstripping the available supply. CyberSeek shows that Maryland has 27,730 job openings and 3,984 of those openings that specifically request GIAC certifications. With more than 63,000 information security workers employed in Maryland, the state currently has over 27,000 openings in the field, with over 13,000 of those positions categorized as being in the "Protect & Defend" domain according to the NICE Cybersecurity Workforce Framework.

Priority 7 calls for efforts to enhance the ways postsecondary education is a platform for ongoing lifelong learning. STI's Bachelor's degree program is, for many students, an early step in a lifelong journey of training and professional development in a field that is constantly evolving. Many BACS graduates continue on to further study through the STI Master's program or our range of Graduate Certificates. With generous lifetime alumni discounts for STI students to renew the professional certifications gained through their degree program, and discounted rates on additional professional training and certifications offered by SANS Institute and GIAC, students are encouraged to keep their knowledge up-to-date, their skills enhanced, and to ensure their best chance of continued career success throughout the entirety of their working lives.

Innovation: Foster innovation in all aspects of Maryland higher education to improve access and student success.

STI has always offered an innovative alternative to the traditional higher education model. With no semesters, monthly rolling admissions, no specific scheduling structures and an entirely flexible approach to delivery modalities, students are empowered to access this innovative and emerging field of study however they feel best fits around their existing commitments.

Priority 8 specifically calls for institutions to "Increase paid real-world experiences (such as internships, externships, work-study opportunities) as a part of new curricula"; this is a key goal of the proposed updates to the BACS curriculum as outlined in this submission, specifically the option for students to source their own suitable external internship for academic credit.

C. Market Supply and Demand in the Region and State

1. Industry, Employment Opportunities, and Expected Level of Entry

It is expected that the overwhelming majority of BACS program graduates will take up employment in the cybersecurity industry, either before or shortly after graduation.

To date, over 72% of STI Bachelor's graduates have been successfully employed in the cybersecurity field before or shortly after completing their program, with over 80% gaining employment in either cybersecurity or a related IT field. Levels of entry vary widely, with BACS graduates' first destinations ranging from "entry-level" cybersecurity analyst positions (although these typically require a higher level of skill, and thus command a higher salary, than a standard entry-level position), up to senior management, director-level and C-suite positions. We expect this wide

range of entry points to continue, as they are so often dependent on the individual's previous professional experience.

It is anticipated that the proposed modifications to the program curriculum, to incorporate a wider range of field experience and portfolio-building opportunities, will enhance the employability of BACS graduates even further.

2. Market Demand

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. In this section, we combine the CyberSeek data with employment projections from the Maryland Department of Labor Licensing and Regulation (DLLR) to estimate the demand for the BACS program in Maryland and in the region.

Cyberseek indicates that there are 469,930 cybersecurity job openings nationally. CyberSeek states that, from May 2023 through April 2024, there were only 85 cybersecurity workers available for every 100 cybersecurity jobs demanded by employers[iii]. In Maryland alone, CyberSeek shows that there are 27,730 job openings and 3,984 of those openings that specifically request GIAC certifications, which are obtained as a degree requirement of the BACS program. These data indicate a high demand not just for cybersecurity workers, but especially for those who have proven, by holding GIAC certifications, that they have the skills to do the job.

3. Anticipated Vacancies

Table C-1: Current Positions and Projected Growth to 2032 in CyberSeek's "Top Cybersecurity Job Titles"[iv]

Job Title	Maryland Positions in 2022	Growth to 2032	Growth in Percent
Information Security Analysts	9291	12,897	38.81%
Computer Systems Analysts	15,524	17,983	15.84%
Network Engineer/Architect	7677	8417	9.64%
Software Developer	34,970	45,887	31.22%

Cybersecurity jobs are already an important part of Maryland's economy, with the state ranking in the top 10 nationwide for net tech employment; employer job postings for tech openings; and tech's economic impact as a percentage of state economy[v]. With the increasing recognition of the vulnerability of critical public and private networks and the need to better protect those networks against constantly evolving threats, it is reasonable to expect that, in conjunction with the State Plan, Maryland will continue to attract additional information security workers and separating military veterans who wish to enter this challenging field. This growth will call for a diverse range of educated technical professionals with a mastery of foundational cybersecurity technologies, and competence in security tools and techniques.

4. Current and Projected Supply of Prospective Graduates

The STI Bachelor's program is projected to significantly increase the number of highly qualified cybersecurity graduates who will be entering the job market over the coming years. Figure C-1 shows the quantity of students successfully completing the STI Bachelor's program from 2022 (when the first BACS students graduated) until the end of 2026 – figures from Q3 2024 onwards are based on the projected completion dates of currently enrolled students. Typical duration is 2 years – so the projections for Q3 and Q4 of 2026 will increase month by month until the end of the current calendar year.

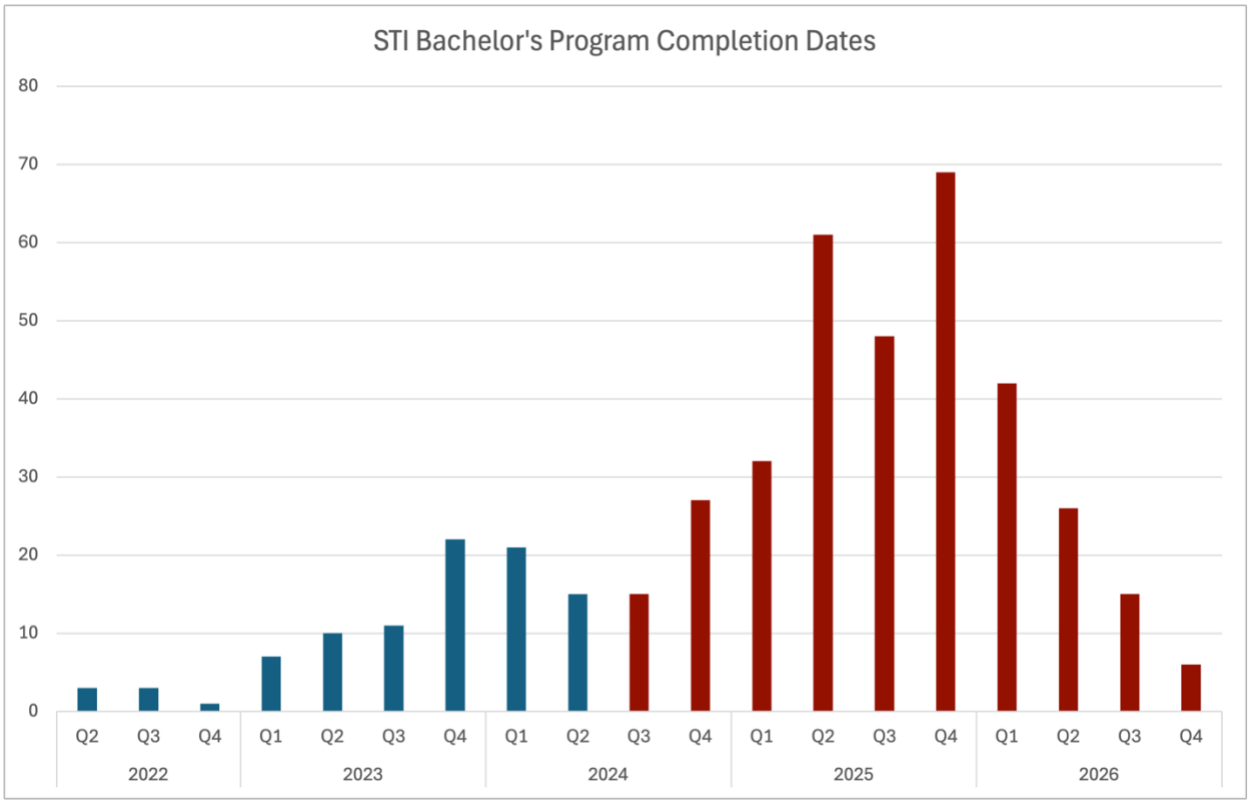

Figure C-1

D. Reasonableness of Program Duplication

This proposal for a "Substantial Modification" to the SANS Technology Institute's BACS program does not alter the number or nature of existing programs related to information security engineering in Maryland, nor how our program relates to those programs. As this substantial modification mainly seeks to increase coherence of the program curriculum and the future employability of its graduates, we do not feel that anything provided in this substantial modification impacts the prior determinations by MHEC regarding program duplication.

Listed here are some key similarities and differences between the STI BACS program (in its proposed updated form) and similar Bachelor's programs offered by other institutions in the state:

Institution	Program Name	Similarities	Differences
Bowie State University	Computer Technology (Cybersecurity)	Includes cybersecurity fundamentals, covering aspects like network security.	STI offer a more in-depth specialism in Applied Cybersecurity, whereas this is a broader tech program.
	Cyber Operations Engineering	Emphasis on cybersecurity operations, infrastructure security, and risk management.	STI emphasizes structured practicums and framework-based competencies, differing from the operations-centric approach.
Capitol Technology University	Construction Info Tech & Cybersecurity	Incorporates core cybersecurity topics, including technical defense methods.	STI focuses on experiential learning and framework-based assessments, unlike the primarily technical approach here.
	Cyber Analytics	Focus on data analytics within the cybersecurity field, similar to data interpretation aspects in STI.	STI's focus includes real-world simulations and hands-on frameworks, unlike analytics-only focus here.
	Cybersecurity	Comprehensive coverage of foundational cybersecurity practices and defensive skills.	STI incorporates structured practicums and portfolio development not included in this curriculum.
	Management of Cyber & Info Technology	Focus on cybersecurity management, complementing STI's management-focused objectives.	STI emphasizes cybersecurity frameworks and practical applications, whereas this program focuses on managerial aspects.
Coppin State University	Cybersecurity Engineering	Focus on cybersecurity fundamentals and engineering principles in cybersecurity.	STI emphasizes communication/reporting skills and framework implementation, which are less highlighted here.
Frostburg State University	Cybersecurity and Information Assurance	Shared focus on core cybersecurity principles and protection methods.	STI includes specific framework-based hygiene assessments and a structured portfolio component, not present here.
Morgan State University	Cybersecurity Intelligence Management	Emphasis on managing cybersecurity risks and threat intelligence analysis.	STI has a stronger focus on hands-on tools and frameworks; this program is more intelligence-oriented.
Mount St. Mary's University	Cybersecurity	General cybersecurity foundation that includes technical skill-building.	STI includes structured experiential elements and portfolio development that this program does not focus on.
Stevenson University	Cybersecurity & Digital Forensics	Emphasis on cybersecurity skill development and investigative methods.	STI includes framework-based learning and general cybersecurity practices, whereas this program has a more definedfocus on forensics.
Univ. of Maryland University College	Cyber Operations	Focus on cybersecurity operations and infrastructure protection.	STI incorporates portfolio development and practical skills in structured practicum settings, which differ here.
	Cybersecurity Management and Policy	Focus on cybersecurity policy and risk management in alignment with NIST.	STI includes hands-on tools and framework-based learning; this program focuses more on policy aspects.
	Cybersecurity Technology	Addresses cybersecurity tools and technologies for protection and defense.	STI emphasizes practical portfolio development and experiential learning, not as prominent in this program.
Univ. of Maryland, College Park	Cyber-Physical Systems Engineering	Emphasis on engineering skills applied to cyber-physical systems.	STI's curriculum includes broader cybersecurity frameworks, while this focuses on physical system security.
University of Baltimore	Cyber Forensics	Covers digital forensics and investigative techniques within cybersecurity.	STI includes structured portfolio-building and cyber hygiene assessments, distinct from the forensic focus here.

The original program proposal provided the below analysis of the similarities and differences between the STI Bachelor's program and other programs awarding Bachelor's degrees in cybersecurity (updated in line with

proposed changes where relevant). This analysis remains accurate in 2024. Key features, such as the integration of GIAC certifications, specialized cybersecurity writing and speaking training, and the Internet Storm Center (ISC) internship, are still not offered by any other cybersecurity bachelor's programs in Maryland. While institutions like the University of Maryland Global Campus (UMGC) have expanded their flexibility and certification preparation, no other programs include GIAC certification as a graduation requirement or offer an equivalent combination of practical and communication-focused training.

1. Similarities and Differences between the BACS Program and Other Programs Awarding Bachelor's Degrees 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.

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

Specific Academic Content of the Program; Evidence of Equivalent Competencies

The BACS program offers students program elements not currently available in any other accredited bachelor's degree program:

1. Nine GIAC certifications

Other colleges in Maryland offer courses designed to prepare students to take cybersecurity certifications, but no other BS program requires graduates to have actually passed advanced cybersecurity certifications as a graduation requirement. Further, none of those programs include passing GIAC certification exams, which require the student to demonstrate hands-on mastery of the skills being evaluated. GIAC certifications are used by the U.S. Department of Defense to qualify employees for advanced cybersecurity roles.

2. Effective security writing and speaking.

Many programs include requirements for business writing. BACS goes further, teaching students how to write the most common security reports, including after-action incident reports, threat reports, malware reports, and several others. It covers elements that should be included in such reports, how to present them, how to illustrate them for maximum impact, and, an area of particular concern in cybersecurity writing, what to leave out. BACS also teaches students how to present cybersecurity information or maximum impact with specific guidance on threat briefings, incident reports, security awareness briefings, and briefings to executives and boards of directors.

3. Guaranteed internship with a globally-recognized information security organization.

Students in the BACS program will participate in a 16-week internship at the Internet Storm Center (ISC). The ISC is the independent research wing of the SANS Technology Institute, with a global network of incident handlers who, similar to the World Health Organization, continuously monitor the internet for emerging threats and attacks. They then conduct analysis of those threats and report their findings out to the world so as to allow organizations to prepare for and respond to new vulnerabilities or attack vectors. This type of experience will prepare BACS students to recognize and respond to incidents in a manner usually unheard of in new, entry-level information security professionals.

Alternative Means of Educational Delivery, including Distance Education

The BACS program gives student the choice between taking each of their advanced cybersecurity courses either remotely or in person in classrooms where they can master the hands-on skills needed to accelerate their careers and build networks of professionals on whom they can call when help is needed. The face-to-face classes are usually accompanied by evening NetWars competitions where students can hone their skills in competition with other students. In contrast, most current cybersecurity bachelor's degree students at Maryland colleges are attending programs that are 100 percent online.

Role and Mission

BACS specifically targets preparing the hunters, tool builders, tech directors, and architects who are critically needed by military and commercial organizations. BACS is not competing with other Maryland cybersecurity programs that are preparing most graduates for security compliance roles or information security analyst roles, or to become security-savvy system and network administrators and help-desk professionals.

2. Admissions Requirements

STI's admission requirements for the Bachelor's program require a 3.0 GPA, in contrast with the largest current Maryland cybersecurity programs that require a 2.0 GPA. This difference allows STI to accelerate the learning process and expect a much higher level of performance from our students. Even more importantly, the BACS admission process includes a psychometric test of cybersecurity aptitude that has proven remarkably reliable in identifying cybersecurity talent, adding to our confidence that BACS graduates will excel in this difficult and important field.

By limiting acceptance to students who have demonstrated strong cyber aptitude, STI can accelerate the student learning process by enabling a focus on rich academic content and advanced competencies.

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

No HBI offers a directly comparable credential that integrates theoretical academics, practical field experience/portfolio building, and professional certifications, although cybersecurity and cyber-related programs are available. Therefore, this proposal for modification should have very little impact on the implementation or maintenance of high-demand programs at HBIs.

The Bachelor's program in Applied Cybersecurity at SANS Technology Institute (STI) is distinct from the programs offered by Maryland's HBIs in several key ways. One of the primary differences is the integration of nine GIAC

certifications into the STI curriculum, which are required for graduation and provide students with industry-recognized credentials. This emphasis on certifications ensures that graduates are equipped with hands-on, practical skills validated through testing. Additionally, STI provides a 16-week internship, giving students practical experience in threat detection and response, which is a unique feature of this program.

The related programs offered by each of Maryland's HBIs are listed below, with a brief summary of how the STI BACS program update could potentially impact their implementation or maintenance.

Coppin State University – Cybersecurity Engineering

Coppin's mission includes providing accessible education in underserved communities. The addition of structured hands-on components in STI's program may appear to raise competition for students seeking practical skills training. However, Coppin's engineering focus will continue to appeal to students interested in a technical, engineering-oriented cybersecurity pathway.

Morgan State University – Cybersecurity Intelligence Management

Morgan's program aligns with its mission to serve diverse populations, emphasizing intelligence management, which is distinct from STI's more broad technical focus. STI's hands-on and framework-based updates may attract additional students, but Morgan's unique focus on intelligence meets a specific high-demand need, sustaining its distinct role in the market.

Bowie State University – Cyber Operations Engineering / Computer Technology (specialization in Cybersecurity)

Bowie's Cyber Operations Engineering program provides a strong focus on operations, preparing students for infrastructure security roles. STI's BACS updates with experiential learning and hands-on tools could appeal to students looking for practical experience, but Bowie's engineering and operations specialization should help maintain its distinct market position. Bowie's Computer Technology and Computer Science programs offer a broad tech foundation, accessible to students seeking general tech skills alongside cybersecurity. STI's program offers similar introductory cybersecurity competencies, however, Bowie's broader tech context may continue to attract students interested in more wide-ranging career pathways.

Overall, while the SANS program has a strong focus on certifications and practical, real-world experience across a range of security disciplines, the HBI programs in Maryland provide more specialized academic pathways in areas such as intelligence management and engineering, catering to students with more specific career aspirations, or offer cybersecurity as a specialization within a broader-ranging degree program.

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

The proposed changes to the BACS program should have no additional impact on the uniqueness and institutional identity or mission of HBIs. The proposal for modification does not seek to introduce any additional curriculum crossover with HBI cybersecurity programs, and does not represent a net change in the number or kind of offerings in undergraduate cybersecurity education within Maryland.

The proposed changes to the BACS program are not expected to impact the unique identities, institutional missions, or educational priorities of Maryland's HBIs, specifically those that offer bachelor's programs in cybersecurity; Coppin State University and Morgan State University.

Coppin State University's Cybersecurity Engineering program emphasizes technical and engineering aspects of cybersecurity, reflecting its mission to serve Baltimore's diverse communities by providing technical education that supports local workforce needs. The BACS modifications, which add structured hands-on experience, and additional core courses in programming and networking, are aligned with STI's mission to address industry standards and skills gaps on a national level. These updates do not interfere with or duplicate Coppin's specialized engineering approach, which remains unique to its identity and mission within its community.

Similarly, Morgan State University's Cybersecurity Intelligence Management program focuses on cybersecurity from an intelligence and risk management perspective. Morgan's mission includes preparing a diverse student body for high-demand fields through a focus on intelligence and risk analysis in cybersecurity. The modifications to the BACS program, particularly the added emphasis on hands-on tools and frameworks, do not overlap with Morgan's intelligence-focused curriculum. Instead, STI's updates target practical skills in cybersecurity defense that support complementary but distinct competencies, allowing Morgan State to retain its unique focus on cybersecurity intelligence.

Additionally, as stated in the original program proposal in 2020, enabling HBIs to become equal partners with STI in overcoming the historical racial imbalance in cybersecurity in the United States can add an important strength to the identity of HBIs. The Bachelor of Science degree is essential to enabling STI to make its undergraduate academic programs available to students in HBIs, regardless of whether they have any previous academic background in cybersecurity. STI welcomes and supports applications from students from HBIs who meet the credit requirements – interested students are invited to take the Cyber Aptitude Test to see whether they are likely to excel in the STI Bachelor's program. Those who score well will be invited to include STI courses and the corresponding certifications in their undergraduate experience, in combination with credit gained from their current institution.

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

1. Establishment of Program and Faculty

Established and approved by MHEC in 2021, the Bachelor's Degree in Applied Cybersecurity is designed to enable community college graduates and others who have completed 70 hours of college courses with a GPA of 3.0 or greater to earn a Bachelor's degree that will position them to get highly paid cybersecurity jobs immediately upon graduation. BACS students develop and demonstrate proficiency in the fundamental technologies and skills that serve as the baseline for all professionals in cybersecurity, as well as gain a mastery of effective written and oral communication of cybersecurity threats, vulnerabilities, and proposed improvements.

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

Dr. Johannes Ullrich

Johannes is Dean of Research at SANS Technology Institute, and also created and manages the SANS Internet Storm Center (ISC) and the GIAC research paper program. In 2000, he founded DShield.org, which is now the data collection engine behind the ISC. His work with the ISC has been widely recognized, and in 2004, Network World named him one of the 50 most powerful people in the networking industry.

Johannes holds a PhD in Physics from SUNY Albany. His daily podcast, listened to by more than 10,000 professionals, summarizes current security news in a concise format.

David Hoelzer

David is the Dean of Faculty at SANS Technology Institute. He is the author of more than twenty days of SANS courseware. He is an expert in a variety of information security fields, having served in most major roles in the IT and security industries over the past 28 years. David was called upon to serve as an expert witness for the Consumer Financial Protection Bureau in a landmark case regarding information security governance within corporations in the financial sector and has previously served as an expert for the Federal Trade Commission for GLBA Privacy Rule litigation and other matters. David has been highly involved in governance at SANS Technology Institute, serving as a member of the Curriculum Committee, Long Range Planning Committee, GIAC Ethics Board, and as Dean of Faculty. As a SANS instructor, David has trained security professionals from organizations including NSA, DHHS, Fortune 500 security engineers and managers, various Department of Defense sites, national laboratories, and many colleges and universities.

Outside of SANS, David is a research fellow in the Center for Cybermedia Research, a research fellow for the Identity Theft and Financial Fraud Research Operations Center (ITFF/ROC), an adjunct research associate of the UNLV Cybermedia Research Lab, a research fellow with the Internet Forensics Lab, and an adjunct lecturer in the UNLV School of Informatics. David has written and contributed to more than 15 peer reviewed books, publications, and journal articles. Currently, David serves as the principal examiner and director of research for Enclave Forensics, a New York/Las Vegas based incident response and forensics company. He also serves as the chief information security officer for Cyber-Defense, an open-source security software solution provider. In the past, David served as the director of the GIAC Certification program, bringing the GIAC Security Expert certification to life.

Joshua Wright

Joshua has worked with hundreds of organizations on attacking and defending complex environments, ethically disclosing significant product and protocol security weaknesses to well-known organizations. He is the author and an instructor for SANS's most popular course, SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling. In addition to being a SANS Faculty Fellow, Joshua serves as the Technical Director of Counter Hack. At Counter Hack he performs penetration testing and red teaming for large and small organizations, developing challenges and learning opportunities for the Holiday Hack Challenge and the NetWars Capture the Flag platform.

Co-author of Hacking Exposed Wireless, Joshua is also an open-source software advocate, whose cutting-edge research has resulted in several software tools commonly used to evaluate the security of widely deployed technology targeting WiFi, Bluetooth, and Zigbee wireless systems, smart grid deployments, and the Android and Apple iOS mobile device platforms.

2. Educational Objectives and Intended Student Learning Outcomes

Through the curriculum review process, it was recommended that the BACS learning outcomes be updated to better reflect some areas that are covered within the program, but not mentioned explicitly in the objectives.

The proposed text for an updated set of program learning outcomes is as follows:-

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

1. Mastery of Foundational Cybersecurity Technologies

- Demonstrate hands-on familiarity with the foundational technologies upon which cybersecurity excellence is built, including computer architecture, networking, programming and scripting, and Linux and Windows operating systems.
- Assemble tools and configure systems and networks to foster resiliency and continuity of operations through attacks.

2. Competence in Security Tools and Techniques

- Demonstrate competence in the use of common security tools to secure all modern operating systems and platforms, assess vulnerabilities and exploits, and excel in the advanced area of specialization they choose.
- Solve real-world cybersecurity problems in simulated but realistic computing environments.

3. Cyber Hygiene and Framework Implementation

- Assess cyber hygiene using the seven key Critical Security Controls.
- Show how those specific controls enable a range of Cybersecurity Frameworks, including NIST.

4. Effective Communication and Reporting

- Communicate security issues effectively to a range of technical and non-technical stakeholders.
- Write security reports and present security briefings competently.

5. Professional Development and Networking

- Start to build a professional network across the information security community.
- Develop a portfolio to showcase cybersecurity achievements and projects.

3. Assessment and Achievement of Learning Outcomes

The learning outcomes have been specifically formulated alongside a formal review of the curriculum to which they relate; therefore, completion of the core requirements of the modified program curriculum directly equates to successful achievement of the learning outcomes.

Students will have access to a public record of their eight GIAC certifications gained through completion of the program, which, alongside their college diploma, will act as formal documentation of achieving objectives 1-3. The portfolio that they will be required to produce as part of the practicum components proposed in this submission will serve as documentation of objectives 4 and 5.

4. Course Requirements and Descriptions

Program Outline

Required Course	Course Name	Credits
BLOCK 1 *(courses must be taken in the specified order)*		**26**
BACS 3275	Foundations: Computers, Technology & Security	6
BACS 3401	Security Essentials	4
BACS 3504	Security Incident Handling and Hacker Exploits	4
BACS 3402	Effective Cyber Writing and Speaking	2
BACS 3373	Introductory Python	3
BACS 3573	Automating Information Security with Python	4
BACS 3001	**Portfolio Practicum (can be completed any time in Block 1):** Experiential Learning through Cyber Challenges (Foundational)	3
BLOCK 2 *(courses can be taken in any order)*		**24**
BACS 3500	Windows Forensic Analysis	4
BACS 3503	Intrusion Detection in-Depth	4
BACS 4999	Elective Course*	3
BACS 4999	Elective Course*	3

BACS 4999	Elective Course*	3
BACS 4499 / BACS 4001	**Field Experience Practicum (choose one option):** Internal Internship/Work Placement (e.g. Apprentice Handler for SANS Internet Storm Center) External Internship (self-sourced professional placement, to be approved by the college)	4
BACS 3002	**Portfolio Practicum (can be completed any time in Block 2):** Experiential Learning through Cyber Challenges (Advanced)	3

Course Descriptions

BACS 3275: Foundations: Computers, Technology, & Security

SANS SEC275 | GIAC GFACT | 6 Credit Hours | 8 Week Course Term

BACS 3275 is purpose-built to provide students with the fundamental technical knowledge and skills that serve as the baseline for all professionals in cybersecurity, reinforcing key concepts with interactive labs. Students establish a core understanding of technology component functions and apply that knowledge to security concepts such as reconstructing a crime from digital evidence or locating exploitable flaws in software and websites. The course ensures a solid mastery of computer, hardware, network, and cybersecurity fundamentals, including the study of operating systems, Windows security tools, Linux, programming with Python and C, advanced Google searches, reconnaissance, virtualization, and encryption. Students explore the inner workings of packets and protocols that allow the internet to function and learn the role of a computer's central processing unit (CPU), how it executes code, its relationship with memory, and the fundamentals of how attackers disrupt intended behavior.

BACS 3401: Security Essentials - Network, Endpoint, and Cloud

SANS SEC401 | GIAC GSEC | 4 Credit Hours | 8 Week Course Term

BACS 3401 is a technically-oriented survey course in which students learn the most effective steps to prevent cyber attacks and detect adversaries. In classes and hands-on labs, students learn the essential information security skills and techniques needed to protect and secure critical information and technology assets, whether on-premise or in the cloud. Student will also learn how to directly apply the concepts learned in developing a winning defensive strategy, all in the terms of the modern adversary.

BACS 3504: Security Incident Handling and Hacker Exploits

SANS SEC504 | GIAC GCIH | 4 Credit Hours | 8 Week Course Term

BACS 3504 is an in-depth focus into the critical activity of incident handling. Students are taught how to manage intrusions by first looking at the techniques used by attackers to exploit a system. Students learn responses to

those techniques, which can be adopted within the framework of the incident handling process to handle attacks in an organized way. The faculty instruction, lab exercises, and exam are coordinated to develop and test a student's ability to utilize the core capabilities required for incident handling today.

BACS 3402: Effective Cyber Writing and Speaking

SANS SEC402 & SEC403 | No GIAC exam | 2 Credit Hours | 8 Week Course Term

BACS 3402 strengthens students' writing and speaking skills. During the first half of the course, students will learn the five "golden elements" of effective reports, briefings, emails, and other cybersecurity writing as well as understand how to pick the best words, structure, look, and tone. The second half of the course gives students the skills to put together an effective security briefing, secure the interest and engagement of their audience, and confidently deliver presentations to a variety of groups.

BACS 3373: Introductory Python

3 Credit Hours | 8 Week Course Term

BACS 3373 is a hands-on course that teaches 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 teaches students how to install and maintain Python programs and modules and to utilize basic Python programming concepts such as functions, IDEs, modules, lists, and basic file input/output.

BACS 3573: Automating Information Security with Python

SANS SEC573 | Additional Labs | GIAC GPYC | 4 Credit Hours | 8 Week Course Term

BACS 3573 teaches student in the pen testing specialization, and other students who want to use the Python programming language, how to enhance their overall effectiveness during information security engagements. Students learn how to apply core programming concepts and techniques learned in other courses through the Python programming language. The course teaches skills and techniques that can enhance an information security professional in penetration tests, security operations, and special projects. Student learning is supported and reinforced by capture-the-flag challenges provided in the *pyWars* lab environment. Students create simple Python-based tools to interact with network traffic, create custom executables, test and interact with databases and websites, and parse logs or sets of data.

BACS 3500: Windows Forensic Analysis

SANS FOR500 | GIAC GCFE | 4 Credit Hours | 8 Week Course Term

BACS 3500 focuses on the critical knowledge of the Windows Operating System that every digital forensic analyst needs to investigate computer incidents successfully. Students learn how computer forensic analysts focus on collecting and analyzing data from computer systems to track user-based activity that can be used in internal investigations or civil/criminal litigation. The course covers the methodology of in-depth computer forensic

examinations, digital investigative analysis, and media exploitation so each student will have complete qualifications to work as a computer forensic investigator helping to solve and fight crime.

BACS 3503: Intrusion Detection In-Depth

SANS SEC503 | Supplemental Materials | GIAC GCIA | 4 Credit Hours | 8 Week Course Term

BACS 3503 delivers the technical knowledge, insight, and hands-on training needed to defend networks with confidence. Students will learn about the underlying theory of TCP/IP and the most used application protocols, such as DNS and HTTP, so that they can intelligently examine network traffic for signs of an intrusion. Daily hands-on exercises suitable for all experience levels reinforce the course book material so that students can transfer knowledge to execution.

BACS 3001: Portfolio Practicum: Experiential Learning through Cyber Challenges (Foundational)

3 Credit Hours | 16 Week Course Term

*Note: this component can be taken concurrently with other courses in Block 1 of the program

This course provides students with hands-on experiential learning opportunities in cybersecurity through participation in national cyber challenges. Students will engage with course content that will enhance their technical skills, critical thinking abilities, and problem-solving techniques essential for success in cybersecurity competitions. Students will compete in a challenge that will provide experience in solving real-world cybersecurity challenges. By strategically incorporating their experience in a cyber challenge into their resume or portfolio, students can effectively demonstrate their skills, knowledge, and passion for cybersecurity to prospective employers.

BACS 3002: Portfolio Practicum: Experiential Learning through Cyber Challenges (Advanced)

3 Credit Hours | 16 Week Course Term

*Note: this component can be taken concurrently with other courses in Block 2 of the program

This course provides students with hands-on experiential learning opportunities in cybersecurity through participation in national cyber challenges at a more advanced level. Students will engage with course content that will enhance their technical skills, critical thinking abilities, and problem-solving techniques essential for success in cybersecurity competitions. Students will compete in a challenge that will provide experience in solving real-world cybersecurity challenges. By strategically incorporating their experience in a cyber challenge into their resume or portfolio, students can effectively demonstrate their skills, knowledge, and passion for cybersecurity to prospective employers.

Field Experience Practicum – students select one option:

4 Credit Hours | 16 Week Course Term

*Note: this component can be taken concurrently with other courses in Block 2 of the program

BACS 4499: Internet Storm Center (ISC) Internship

Much like the World Health Organization and its global disease monitoring network, the SANS Technology Institute, through its research wing in the Internet Storm Center (ISC), maintains and operates the world's leading global cyber threat detection network.

The ISC depends on continuous input from a series of DShield sensors and web application honeypots. Of course, all that collected data accomplishes nothing if it is not processed, interpreted, analyzed and very quickly reported to the global information security community. This is the role of the ISC handlers, the frontline personnel of global threat detection, whose main task is to take all the input received into the ISC and turn it into "diaries" (https://isc.sans.edu/diaryarchive.html).

This internship as an Apprentice Handler will provide a student with a continuous opportunity over the course of 16 weeks to observe emerging threats, to analyze and report upon those threats, and to gain experience under the mentorship of a Handler or Senior Handler. This hands-on, real-world experience will prepare the student for a first professional cybersecurity role in a way that few other programs can. That experience will include not only a deepening of practical understanding of real-world technical issues, but also the ability to effectively write and communicate about those issues.

BACS 4001: External Internship

Students may source their own external internship, and submit this to be considered for academic credit over a 16-week period. Suitable internships must consist of a minimum of 80% cybersecurity-related work, and be signed off by a designated professional supervisor at the organization.

In addition to any assignments required by the internship provider, students must complete regular check-ins with their assigned college Career Specialist, and will be required to submit a minimum of 2 reflective assignments.

BACS 4999: Elective (x3)

3 Credit Hours | 8 Week Course Term

Students choose 3 electives from an approved list of courses. Electives can be taken within one specialist area, or chosen from across the full range. Please see the current list of acceptable technical elective courses and their full descriptions in Appendix II.

5. General Education Requirements

Students are required to have completed 70 General Education credits before admittance.

6. Specialized Accreditation/Certification Requirements

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

7. Contract with Another Institution or Non-Collegiate Organization

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

A copy of the full Memorandum of Understanding between The SANS Technology Institute ("STI") and The Escal Institute of Advanced Technologies ("SANS") is provided in Appendix I.

8. Enrolled Student Communications

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

9. Prospective Student Communications

BACS program requirements and student services are found on our website at www.sans.edu. All marketing materials will be updated with the new version of the curriculum, and any students in the admissions pipeline when the curriculum updates are approved will be personally notified of any changes from the previously approved curriculum version.

H. Adequacy of Articulation

SANS Technology Institute's BACS program does allow for the transfer or waiver of prior SANS courses and/or GIAC examinations completed through our own programs or directly through SANS.org. STI does not accept transfer coursework from other academic programs. Thus, no articulation agreements currently exist and none are anticipated.

I. Adequacy of Faculty Resources

1. Program Faculty

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

Faculty for this program includes the following individuals:

Faculty: Johannes Ullrich

Appointment Type: Permanent

Status: Full-time

Terminal Degree Title and Field: Ph.D. in Physics

Academic Rank/Title: Professor/Fellow

Course taught: BACS 4999

Professional Certifications: GCIA, GWEB, GNFA, GMON

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

Faculty: David Hoelzer

Appointment Type: Permanent

Status: Full-time

Terminal Degree Title and Field: M.S. In Computer Science

Academic Rank/Title: Professor/Fellow

Course taught: BACS 3503

Professional Certifications: GCIA, GSNA, GSE, G2700, CCE, GSLC

David is the Dean of Faculty at STI. He is the author of more than twenty days of SANS courseware. He is an expert in a variety of information security fields, having served in most major roles in the IT and security industries over the past twenty-five years. Recently, David was called upon to serve as an expert witness for the Consumer Financial Protection Bureau in a landmark case regarding information security governance within corporations in the financial sector and has previously served as an expert for the Federal Trade Commission for GLBA Privacy Rule litigation and other matters. David has been highly involved in governance at SANS Technology Institute, serving as a member of the Curriculum Committee, Long Range Planning Committee, GIAC Ethics Board, and as Dean of Faculty. As a SANS instructor, David has trained security professionals from organizations including NSA, DHHS, Fortune 500 security engineers and managers, various Department of Defense sites, national laboratories, and many colleges and universities.

Faculty: Mark Baggett

Appointment Type: Permanent

Status: Full-time

Terminal Degree Title and Field: M.S. in Information Security Engineering

Academic Rank/Title: Associate Professor/Senior Instructor

Course taught: BACS 3573

Professional Certifications: GSEC, GCIH, GCIA, GPEN, GCPM, GWAPT, GXPN, GPYC, GSE

Mark's infosec career spans nearly 30 years with 15 of those years spent teaching for SANS. Mark is currently a faculty fellow for SANS and an independent consultant through his company Indepth Defense providing forensics, incident response, and penetration testing services. Mark served as the technical advisor to the DoD for SANS from 2011 until 2024, where he assisted various government organizations in the development of information security capabilities. Today, he is the Chief Technology Officer for the Internet Storm Center.

Table I-1 shows a full list of faculty members for the core courses within the BACS curriculum, including their academic credentials.

Table I-1

Name	Degree	Field of Degree	Academic Title Rank	Status	Course(s)
James Lyne	MS	Information Security	Certified Instructor	Full-time	BACS 3275
Bryan Simon	GSE, CISSP	Information Security	Senior Instructor	Full-time	BACS 3401
Joshua Wright	BSIS	Information Science	Faculty Fellow	Full-time	BACS 3504
Lenny Zeltser	MS	Information Security	Faculty Fellow	Adjunct	BACS 3402
Mark Baggett	MS	Information Security Engineering	Associate Professor/ Faculty Fellow	Full-time	BACS 3373 BACS 3573
Rob Lee	BSIS	Engineering, Military Strategy	Professor/ Faculty Fellow	Full-time	BACS 3500
David Hoelzer	MS	Computer Science	Professor/ Faculty Fellow	Full-time	BACS 3503
Johannes Ulrich	PhD	Physics	Professor/ Faculty Fellow	Full-time	BACS 4499

2. Faculty Recruitment and Development

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

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

Figure I-1

Mentor / TA

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

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

Community Instructor / TA

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

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

Trial Instructor / Supervised Instruction / TA

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

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

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

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

Certified Instructor

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

Certified Instructors, as Adjunct Faculty, are also expected to display the aspects of a Scholar/Practitioner as discussed on page 11. As a Certified Instructor/Adjunct Faculty it is also expected that the individual will maintain the high caliber of instructor required of a Master Teacher and, as such, will be subject to the same periodic assessment by the Program Directors and Professor of Practice.

Senior Instructor

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

Faculty members who consistently achieve the highest evaluated ratings and who additionally have more than 240 course contact hours each year may qualify as Senior Instructors. Senior Instructors typically have additionally

demonstrated significant leadership within the community of practice, perhaps through the development of course material used within the college or an affiliated entity.

Faculty Fellow

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

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

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

Faculty Development Opportunities

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

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

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

Faculty who participate in our 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 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.

J. Adequacy of Library Resources

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

information services, our current and future students have continuous access to the following list of primary resources:

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

K. Adequacy of Physical Facilities, Infrastructure and Instructional Equipment

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

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

L. Adequacy of Financial Resources with Documentation

1. Table 1: Program Resources

Resource Categories	2025	2026	2027	2028	2029
Reallocated Funds	0	0	0	0	0
Tuition/Fee Revenue (c + g)	4,620,000	5,082,000	5,588,000	6,149,000	6,765,000
Number of F/T Students	420	462	508	559	615
Annual Tuition/Fee Rate	11,000	11,000	11,000	11,000	11,000
Total F/T Revenue (a x b)	4,620,000	5,082,000	5,588,000	6,149,000	6,765,000
Number of P/T Students	0	0	0	0	0
Credit Hour Rate	0	0	0	0	0
Annual Credit Hour Rate	0	0	0	0	0
Total P/T Revenue (d x e x f)	0	0	0	0	0
Grants, Contracts & Other External Sources	0	0	0	0	0
Other Sources	0	0	0	0	0
TOTAL (Add 1-4)	**4,620,000**	**5,082,000**	**5,588,000**	**6,149,000**	**6,765,000**

2. Table 2: Expenditures

Expenditure Categories	2025	2026	2027	2028	2029
Faculty (b + c below)	1,653,100	1,875,035	2,002,850	2,193,260	2,417,780
# FTE	N/A	N/A	N/A	N/A	N/A
Total Salary	991,860	1,125,021	1,201,710	1.315,956	1,450,668
Total Benefits	661,240	750,014	801,140	877,304	967,112
Admin. Staff (b + c below)	352,800	386,400	428,400	470,400	512,400
# FTE	4.2	4.6	5.1	5.6	6.1
Total Salary	252,000	276,000	306,000	336,000	366,000
Total Benefits	100,800	110,400	122,400	134,400	146,400
Support Staff (b + c below)	0	0	0	0	0
# FTE	0	0	0	0	0
Total Salary	0	0	0	0	0
Total Benefits	0	0	0	0	0
Technical Support and Equipment	0	0	0	0	0
Library	0	0	0	0	0
New or Renovated Space	0	0	0	0	0
Other Expenses	50,000	55,000	61,000	66,500	73,500
TOTAL (Add 1-7)	**2,055,900**	**2,261,490**	**2,492,250**	**2,730,160**	**3,003,680**

M.Financial Data Narrative

Table 1: Resources

Re-allocated Funds
N/A

Tuition and Fee Revenue

The tuition projection builds upon current student enrollment headcount and admissions trends for this program. The projection also incorporates current retention data and average times to graduation.

Grants and Contracts
N/A

Other Sources
N/A

Total Year
N/A

Table 2: Expenditures

Faculty

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

Administrative and Support Staff

The STI undergraduate programs currently operate at a ratio of students to administrative staff ratio of 100:1. Average salary and benefit information is reflective of our current cost experience and market expectations.

Equipment, Library, New and/or Renovated Space

The BACS program update will not require any additional equipment, library facilities, or any new and/or renovated space. We have ample capacity in our existing facilities, residential institutes, online platform capacity, and offices.

Other Expenses

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

N. Adequacy of Provisions for Evaluation of Program

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

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

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

3. **To evaluate program outcomes,** STI tracks all graduates and asks them (and when possible, their employers) annually for feedback on how well the program worked for them and how it might be improved. Additionally, STI has implemented its formal Learning Outcomes Assessment Plan, as endorsed by the MSCHE evaluation team. Under this plan, each program undergoes a formal review by an evaluation team comprised of subject matter experts every five years. This review process will ensure alignment of (1) course outcomes to program learning objectives, of (2) program learning objectives to any capstone requirements, and of (3) both program learning objectives and capstone requirements to a survey of industry requirements. This request for substantial change is based upon the BACS program review in 2024.

O. Consistency with the State's Minority Student Achievement Goals

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

P. Relationship to Low Productivity Programs Identified by the Commission

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

Q. Adequacy of Distance Education Programs

1. Eligibility to Provide Distance Education

STI was approved by Middle States to deliver more than 50 percent of our credit via distance modalities following submission of a Substantive Change Request in 2014.

R. Compliance with C-RAC Guidelines

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

The two distance learning modalities available to students to complete the SANS technical course component are OnDemand and Live Online. 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 Live Online delivery modality allows students to participate in a course being offered through the in-person modality, but from their location of choice, enabled through a digital learning management system. Students meet during the same time the in-person course meets. They can participate in classroom lectures by seeing and hearing the instructor, in addition to asking questions and participating in classroom discussion.

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

1. Curriculum and instruction

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

STI faculty members design all distance learning programs.

2. Role and mission

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

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

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

The appropriateness of the technology STI uses for distance education has evolved over more than 15 years to be optimized for meeting the active learning needs of full-time working professionals, and it been assessed and approved by STI faculty. But that is not the end of the development process. The distance learning technology is continuously evaluated through surveys completed by every one of the more than 3,000 cybersecurity professionals using it each day. If a course is not helping students master the key learning objectives, we hear about it quickly and fix the problems.

3. Faculty support

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

Faculty who participate in our OnDemand and Live Online 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 Live Online to students) employing an assistant in the room who participates in the class on behalf of distance students by flagging the instructor's attention when questions are asked or issues are raised by virtual students.

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

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

Instructor Guidelines for SANS Live Online Classes

What to Expect

During a SANS Live Online 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 Zoom 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.

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 Zoom 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 Live Online class is to always **remember that you are teaching remote students; keep them engaged** by promptly responding to their questions and periodically addressing them directly.

Advance Planning

1. The 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 Live Online will be shipped to the Live Online location prior to class.

3. The Live Online support team will be setting up the audio equipment and test the setup with you. This test is critical to the success of the Live Online 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 Live Online team will introduce you to the virtual moderator who will be working the classroom. This moderator is a SANS employee who is there to assist with the running of Zoom, running labs, and assisting with student questions. Many instructors prefer that the moderator relays questions from the virtual students by raising his or her hand and reading the question.

Audio Tips

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

7. Leave your wireless microphone on at all times, but turn off your Zoom audio during breaks. To do this, simply ask your on-site moderator to mute you on the class 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 Live Online 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 Zoom’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 Zoom 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 Zoom 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.

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

SANS Live Online is supported by the Onsite team. The Onsite team provides most of the support during class. While you are teaching you will have one or more moderators in the virtual classroom to provide assistance with labs and logistics.

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

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

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

source for advanced security research projects that analyze attack patterns and how fast worms spread through the Internet.

- SANS Web Briefings held several times a month feature SANS faculty and other security experts providing up-to-date web briefings for SANS alumni on new threats seen at the Internet Storm Center, new technologies that are emerging, and analysis of security trends.

5. Students and Student Services

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

- Curriculum information is posted, in detail, at the SANS.EDU website at https://www.sans.edu/academics/
- Course and degree requirements are posted online in the STI Course Catalog at https://www.sans.edu/about/student-consumer-information/
- The nature of faculty/student interaction are described on our website at https://www.sans.edu/course-delivery-options/
- Assumptions about technology competence and skills are posted at our Admissions website at https://www.sans.edu/admissions/undergraduate/
- Technical equipment requirements are posted with individual courses at the SANS course website.
- Learning management systems information is posted in detail at https://www.sans.org/frequently-asked-questions/?categories=ondemand-training
- The availability of academic support services and financial aid resources is posted at https://www.sans.edu/students/services, and in the "Student Services" section of the Student Handbook - https://www.sans.edu/downloads/sti-student-handbook.pdf
- Costs and payment policies are posted at https://www.sans.edu/admissions/tuition

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

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

Quantified measures of specific sub-processes with student management were also high, with over 95% of respondents saying they were "Satisfied" with each of the operational elements, as shown in Figure P-1.

Figure R-1: Student Satisfaction with Student Management as Reported in the 2023 Student Experience Survey

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

Our BACS students have demonstrated a strong aptitude for cybersecurity through the aptitude assessment they are required to take as part of the admissions process. They are also required to have at least 70 general education credits from another accredited institution, so should be well acquainted with the rigours of higher education by the time they commence this program. Thus, they have the needed background, knowledge, and technical skills to use the distance learning modalities.

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

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

5. Commitment to support

c) ***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.

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

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

6. Evaluation and assessment

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

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

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

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

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

Ultimate student achievement in the BACS 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 P-2, the GIAC test scores in distance learning are essentially identical to scores of students who used live, in-person residential training programs:

Table R-2: 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 BACS program, by delivery modality.

Appendix I. Contracts with Related Entities

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

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

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

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

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

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

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

Memorandum of Understanding

between

The SANS Technology Institute ("STI")

and

The Escal Institute of Advanced Technologies ("SANS")

Agreement Published Date: June 1st, 2023

Agreement Period of Performance: June 1st, 2023 – December 31st, 2025

Purpose

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

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

Vision

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

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

Mission

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

Scope

The SANS Institute will provide access for STI students, in all delivery modalities, to the Technical courses offered by the SANS Institute that are a part of STI's course curricula, including, Course Maintenance, Presentation of this course material , and Educational Residency services for the SANS Technology Institute. The SANS Institute shall

provide policy-compliant management of Accounting & Finance, Bursar & Registration, Human Resource, Marketing, and Information Technology infrastructures for STI.

Hours of Operations

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

Service Expectations

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

Accounting and Finance

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

Bursar & Registration

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

Human Resources

Process	Service Expectation	Service Metric
Benefits	Provide benefits which are in the best interest of the employees and employer	Annual survey of employees will show that major benefits of interest are being adequately provided
Payroll	Assure timely payroll and employee reviews	All bimonthly payrolls will be made on the 15th and final days of the month
HR services	Manage HR service to ensure receipt by employees	HR services are provided for in a timely manner as measure in annual survey and changes are communicated and enforced

Marketing

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

Information Technology

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

Technical Course Maintenance & Presentation

Process	Service Expectation	Service Metric
Currency of content	Make available for use by STI Faculty any and all technical content developed by the SANS Institute	Content is reviewed at least semi-annually for currency with existing malicious capabilities and mitigation theory and strategy
Quality of content and presentations	Assist through all means necessary and available the delivery of STI faculty and lab instruction in a high-quality fashion	SANS Institute will make available all performance ratings derived from students on STI courses or faculty

Educational Residency

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

Service Constraints

- ***Workload -*** Increases in workload, such as back log due to power outages or fiscal year end closing, may result in temporary reduction of service level delivery.

- ***Conformance Requirements -*** Finance policy changes and Internal Revenue regulations may alter procedures and service delivery timeframes.

- ***Dependencies -*** Achievement of the service level commitment is dependent upon student and employee compliance with the policies and procedures of the STI enterprise.

Terms of Agreement

The term of this agreement is June 1, 2023 - December 31, 2025. This Agreement may be cancelled only by STI, at its sole discretion.

STI and SANS will, in November of each year, conduct analysis on the impact of year-to-date payments in order to assess the financial health and performance of STI and will initiate appropriate adjustments to ensure the health of STI and its ability to properly support students and the overall mission of STI to recruit, enroll, and graduate information security practitioners and leaders. Any such adjustment will be approved by the STI Financial Committee.

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 Provost 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 $1,900 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).
- STI will pay SANS $315 for each instance when an STI student registers for a short SANS class (2- or 3-day course) as part of an STI course, regardless of the chosen delivery modality (live event or online).
- STI will pay SANS $675 for each instance when an STI student registers for SEC 275, Foundations, as part of an STI course, regardless of the chosen delivery modality (live event or online).
- STI will pay amounts to SANS, monthly in arrears, to reflect any directly allocated expenses by SANS personnel in support of STI business according to this services agreement (specifically including the result of any time allocation procedures as determined by SANS accounting department)
- • STI will pay an amount to SANS, monthly in arrears, to reflect its pro-rata share of SANS' otherwise unallocated costs for Accounting & Finance, Bursar, Human Resource, Marketing and Information Technology, and related administrative services, in proportion to its share of revenue relative to SANS revenue also sharing in this services pool.

Agreed to on behalf of STI:	Agreed to on behalf of SANS:
_____	_____
Eric A. Patterson	Peggy Logue
Provost	Chief Financial Officer
SANS Technology Institute	SANS Institute
_____	_____
Date:	Date:

Appendix A:

Product Type	**MOU Fee**
Long Course	$1900
Short Course	$315
SEC 275 Foundations	$675
Cyber Ranges	$0

If **ACSCFT** registration code is used, no MOU fee is charged.

Appendix II: Technical Elective Course Options

The following are current approved technical elective courses. Students in the BACS program must choose 3 courses from the list of approved technical electives.

ACS 4410: Security Essentials for Industrial Control Systems

SANS ICS410 | GIAC GICSP

ACS 4410 is designed to help traditional IT personnel fully understand the design principles underlying control systems and how to support those systems in a manner that ensures availability and integrity. In parallel, the course addresses the need for control system engineers and operators to better understand the important role they play in cybersecurity. Students will learn the language, the underlying theory, and the basic tools for industrial control system security in setting across a wide range of industry sectors and applications.

Prerequisites: BACS 3504

ACS 4450: Blue Team Fundamentals: Security Operations and Analysis

SANS SEC450 | GIAC GSOC

ACS 4450 provides students with technical knowledge and key concepts essential for security operation center (SOC) analysts and new cyber defense team members. By providing a detailed explanation of the mission and mindset of a modern cyber defense operation, this course will jumpstart and empower those on their way to becoming the next generation of blue team members.

Prerequisites: BACS 3504

ACS 4456: Essentials of NERC Critical Infrastructure Protection

SANS ICS456 | GIAC GCIP

ACS 4456 empowers students with knowledge of the what and the how of the Critical Infrastructure Protection (CIP) Reliability Standards versions 5/6/7. The course addresses the role of the Federal Energy Regulatory Commission (FERC), North American Electric Reliability Corporation (NERC), and Regional Entities, provides multiple approaches for identifying and categorizing BES Cyber Systems, and helps asset owners determine the requirements applicable to specific implementations.

Prerequisites: BACS 3504

ACS 4497: Practical Open-Source Intelligence (OSINT)

SANS SEC497 | GIAC GOSI

ACS 4497 is a foundational course in open-source intelligence (OSINT) gathering that teaches students practical, real-world tools and techniques to help them perform OSINT research safely and effectively. The course not only covers critical OSINT tools and techniques, it also provides real-world examples of how they have been used to solve a problem or further an investigation. Hands-on labs based on actual scenarios provide students with the opportunity to practice the skills they learn and understand how those skills can help in their research.

Prerequisites: BACS 3504

ACS 4488: Cloud Security Essentials

SANS SEC488 | GIAC GCLD

ACS 4488 covers Amazon Web Services, Azure, Google Cloud, and other cloud service providers (CSPs). Like foreign languages, cloud environments have similarities and differences, and this course will introduce students to the language of cloud security. Upon completion of this course, students will be able to advise and speak about a wide range of cybersecurity topics and successfully navigate the challenges and opportunities presented by cloud service providers.

Prerequisites: BACS 3504

ACS 4498: Battlefield Forensics & Data Acquisition

SANS FOR498 | GIAC GBFA

ACS 4498 provides the necessary skills to identify the many and varied data storage mediums in use today and how to collect and preserve this data in a forensically sound manner despite how and where it may be stored. It covers digital acquisition from computers, portable devices, networks, and the cloud. It then teaches the student Battlefield Forensics, or the art and science of identifying and starting to extract actionable intelligence from a hard drive in 90 minutes or less.

Prerequisites: BACS 3504

ACS 4508: Advanced Digital Forensics and Incident Response

SANS FOR508 | GIAC GCFA

ACS 4508 teaches students the necessary capabilities for forensic analysts and incident responders to identify and counter a wide range of threats within enterprise networks. This course is constantly updated and addresses today's incidents by providing hand-on forensics tactics and techniques that elite responders are successfully using in real-world breach cases.

Prerequisites: BACS 3504

ACS 4510: Public Cloud Security

SANS SEC510 | GIAC GPCS

ACS 4510 provides students with an in-depth understanding of the inner workings of the most popular public cloud providers: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). Students will learn industry-renowned standards and methodologies, such as the MITRE ATT&CK Cloud Matrix and CIS Cloud Benchmarks, then apply that knowledge in hands-on exercises to assess a modern web application that leverages the cloud native offerings of each provider. Through this process students will learn the philosophies that undergird each provider and how these have influenced their services.

Prerequisites: BACS 3504

ACS 4511: Continuous Monitoring and Security Operations

SANS SEC511 | GIAC GMON

A new proactive approach to security is needed to enhance the capabilities of organizations to detect threats that will inevitably slip through their defenses. ACS 4511 teaches this new proactive approach and strengthens student's skills to undertake that proactive approach. The Defensible Security Architecture, Network Security Monitoring (NSM)/Continuous Diagnostics and Mitigation (CDM)/Continuous Security Monitoring (CSM) taught in this course will help students best position their organization or Security Operations Center (SOC) to analyze threats and detect anomalies that could indicate cybercriminal behavior.

Prerequisites: BACS 3504

ACS 4515: ICS Visibility, Detection, and Response

SANS ICS515 | GIAC GRID

ACS 4515 will help students gain visibility and asset identification in Industrial Control System (ICS)/Operational Technology (OT) networks, monitor for and detect cyber threats, deconstruct ICS cyber attacks to extract lessons learned, perform incident response, and take an intelligence-driven approach to executing a world-leading ICS cybersecurity program to ensure safe and reliable operations.

Prerequisites: BACS 4410

ACS 4522: Defending Web Applications Security Essentials

SANS SEC522 | GIAC GWEB

ACS 4522 covers the OWASP Top 10 and provides students with a better understanding of web application vulnerabilities, enabling them to properly defend organizational web assets. Mitigation strategies from an infrastructure, architecture, and coding perspective are discussed alongside real-world implementations that really work. The testing aspect of vulnerabilities is also covered so students can ensure their application is tested for the vulnerabilities discussed in class.

Prerequisites: BACS 3504

ACS 4540: Cloud Security and DevOps Automation

SANS SEC540 | GIAC GCSA

ACS 4540 provides security professionals with a methodology for securing modern Cloud and DevOps environments. Students learn how to implement over 20 DevSecOps Security Controls for building, testing, deploying, and monitoring cloud infrastructure and services. Immersive hands-on labs ensure students not only understand theory, but how to configure and implement each security control. By embracing the DevOps culture, students will walk away battle tested and ready to build an organization's Cloud & DevOps Security program.

Prerequisites: BACS 3504

ACS 4542: Web App Penetration Testing & Ethical Hacking

SANS SEC542 | GIAC GWAPT

With in-depth, hands-on labs and high-quality course content, ACS 4542 helps students move beyond push-button scanning to professional, thorough, and high-value web application testing. This enables students to demonstrate the impact of inadequate security that plagues most organizations' websites. The addition of a series of enrichment exercises that strengthen students' ability to work in Python and understand how the networks and operating systems enable web attacks to succeed so as to become even more insightful penetration testers.

Prerequisites: BACS 3504

ACS 4560: Enterprise Penetration Testing

SANS SEC560 | GIAC GPEN

Both the offensive teams and defenders of an enterprise have the same goal: keep the real bad guys out. Every organization needs skilled information security personnel who can find vulnerabilities and mitigate their effects, and this entire course is specifically developed to get students ready for that role. ACS 4560 is designed to strengthen penetration testers and further add to their skillset. The course is also designed to train system administrators, defenders, and others in security to understand the mindset and methodology of a modern attacker. Students will learn how to plan, prepare, and execute a penetration test in a modern enterprise. Using the latest penetration testing tools, students will undertake extensive hands-on lab exercises to learn the methodology of experienced attackers and practice their skills.

Prerequisites: BACS 3504

ACS 4566: Implementing and Auditing the Critical Security Controls In-Depth

SANS SEC566 | GIAC GCCC

Cybersecurity attacks are increasing and evolving so rapidly that is more difficult than ever to prevent and defend against them. ACS 4566 will help students to ensure that their organization has an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches. As threats evolve, an organization's security should too. Standards based implementation takes a prioritized, risk-based approach to security and shows students how standardized controls are the best way to block known attacks and mitigate damage from successful attacks.

Prerequisites: BACS 3504

ACS 4575: Mobile Device Security and Ethical Hacking

SANS SEC575 | GIAC GMOB

ACS 4575 helps students resolve their organization's struggles with mobile device security by equipping then with the skills needed to design, deploy, operate, and assess a well-managed secure mobile environment. From practical policy development to network architecture design and deployment, and mobile code analysis to penetration testing and ethical hacking, this course teaches students to build the critical skills necessary to support the secure deployment and use of mobile phones and tablets in their organization.

Prerequisites: BACS 3504

ACS 4588: Cloud Penetration Testing

SANS SEC588 | GIAC GCPN

ACS 4588 equips students with the latest in cloud-focused penetration testing techniques and teaches them how to assess cloud environments. The course dives into topics like cloud-based microservices, in-memory data stores, serverless functions, Kubernetes meshes, and containers, as well as identifying and testing in cloud-first and cloud-native applications. Students will also learn specific tactics for penetration testing in Azure and Amazon Web Services, particularly important given that AWS and Microsoft account for more than half the market.

Prerequisites: BACS 3504

ACS 4595: Applied Data Science and AI/Machine Learning for Cybersecurity Professionals

SANS SEC595 | GIAC GMLE

ACS 4595 is squarely centered on solving information security problems. This course covers the necessary mathematics theory and fundamentals students absolutely must know to allow them to understand and apply the machine learning tools and techniques effectively. The course progressively introduces and applies various statistic, probabilistic, or mathematic tools (in their applied form), allowing students to leave with the ability to use those tools. The hands-on projects provide a broad base from which students can build their own machine learning solutions. This course teaches how AI tools like ChatGPT really work so that students can intelligently discuss their potential use by organizations and how to build effective solutions to solve real cybersecurity problems using machine learning and AI.

Prerequisites: BACS 3504

[i] Source: https://www.cyberseek.org/heatmap.html (accessed August 22, 2024)
[ii] Source: https://www.comptia.org/content/research/state-of-the-tech-workforce (accessed August 22, 2024)
[iii] Source: https://www.cyberseek.org/ (accessed August 22, 2024)
[iv] Source: https://www.dllr.state.md.us/lmi/iandoproj/maryland.shtml (accessed August 22, 2024)

[v] Source: https://www.comptia.org/content/research/state-of-the-tech-workforce (accessed August 22, 2024)