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

May 26, 2020

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

Dear Dr. Fielder,

The SANS Technology Institute is pleased to submit the attached proposal to create a new Purple Security Operations post-baccalaureate certificate program. As the first program of its kind, in Maryland or anywhere, this graduate certificate will formalize an emerging best practice in the information security industry by providing aspiring full spectrum leaders the education and skills needed to lead combined teams of blue team defenders and red team penetration testers.

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.

Alan Paller
President
SANS Technology Institute

PROPOSAL FOR A POST-BACCALAUREATE CERTIFICATE IN PURPLE SECURITY OPERATIONS

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.

- (X) 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:	Payment Type:	Payment Amount:	Date Submitted:
( ) Yes (X) No	( ) R*STARS ( ) Check		

Department Proposing Program	SANS Technology Institute	
Degree Level and Degree Type	Post-baccalaureate Certificate	
Title of Proposed Program	Purple Security Operations	
Total Number of Credits	15	
Suggested Codes	HEGIS: 5199	CIP: 11.1003
Program Modality	(X) On-campus	( ) Distance Education (*fully online*)
Program Resources	(X) Using Existing Resources	( ) Requiring New Resources
Projected Implementation Date	(•) Fall ( ) Spring (X) Summer	Year: 2020
Provide Link to Most Recent Academic Catalog	URL: https://www.sans.edu/downloads/STI-2019-Graduate-Course-Catalo	
Preferred Contact for this Proposal	Name: Eric Patterson	
	Title: Executive Director	
	Phone: (440) 321-3040	
	Email: epatterson@sans.edu	
President/Chief Executive	Type Name: Alan Paller	
	Signature:	Date: 26 May 2020
	Date of Approval/Endorsement by Governing Board: 22 May 2020	

Revised 4/2020

Table of Contents

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

1. Program Description

The SANS Technology Institute (STI) proposes to launch a new program leading to a Post-Baccalaureate Certificate in Purple Security Operations. The proposed SANS Technology Institute graduate certificate program is a 15-credit hour program with a cohesive set of learning outcomes focused on teaching blue and red applied concepts, skills, and technologies used in a merged fashion in the current best practice known as purple operations, or purple teams. This program would be intended for experienced information security practitioners who are interested in rounding out their blue and red skills so as to be able to effectively operate and lead at the intersection of those domains.

Purple Security Operations graduate certificate students will complete two required core courses, two elective courses, and a capstone course, earning five industry-recognized GIAC certifications.

A full course listing with course descriptions is provided in Section G.

The proposed program will be delivered using the same live classroom settings, online modalities, and student management systems that are currently employed in delivering STI's five other graduate certificate programs. Purple Security Operations graduate certificate students will have, just as is true for all STI students, access to mentors and assistants online, will interact with each other online and at live events, and will take their exams required to complete the courses live at a proctored testing center or through remote proctoring sessions. For admission to the program, students must have completed a bachelor's degree at an accredited institution with a cumulative GPA of 2.8, and must have at least one year of experience in information technology or information security. Further details on the admission standards and process to STI graduate certificate programs can be found online at https://www.sans.edu/admissions/certificates.

2. Relation to STI Mission and Strategic Goals

The proposed graduate certificate program aligns well with STI's mission and vision.

Our mission calls for us to graduate "technically-skilled leaders to strengthen enterprise and global information security" who can, according to our vision, "design, champion, and manage the implementation and ongoing operation of state-of-the-art, enterprise-level cyber defenses" as they fulfill our institutional goal of "enabling private and public sector enterprises of the United States and its allies to preserve social order and to protect their economic rights and military capabilities in the face of cyber attacks."

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

1. Critical Need for the Purple Security Operations Program

Historically, the information security industry has tended to compartmentalize defensive, or blue team, and penetration testing, or red team, activities. The natural synergy and efficiency gained by bringing these two sets of activities and specialists into closer alignment has resulted in the expanding adoption of purple teams, which combine these conceptually oppositional approaches and skillsets for the improved defense of enterprise networks. As the information security industry continues to evolve and mature, we are already seeing that the concept of purple teams and operations is becoming more familiar and more widely embedded into enterprise operations. A Dark Reading article from the summer of 2019 describes purple operations as a "fast-rising cybersecurity trend" which has "has changed the way many organizations conduct their penetration tests by providing a more collaborative approach to old-fashioned Red Team vs. Blue Team methodology."[1] This ongoing trend will logically require leaders who are not just experienced in both domains, but who specifically possess a deep understanding of how to implement, develop, integrate, orchestrate, and lead purple teams and operations in increasingly sophisticated ways.

The proposed Purple Security Operations graduate certificate program aligns directly with Maryland Core Goal #6: Cybersecurity and Critical Infrastructure Protection.[2] This goal states that,

All critical government computer networks and systems should be protected from cyber attack. Critical private sector entities including utilities should be included in cyber security planning, training, and exercising. The State should be able to effectively respond to cyber incidents involving public and private networks that impact the well-being of Maryland residents, businesses, and the ability of the State to provide essential government services.

Consisting of four sub-goals, each with a specific focus, Maryland's preparations to respond to cyber incidents have been integrated into the State's intelligence fusion center.[3] This intelligence fusion center is, itself, a valid analog of the very concept of purple operations within the domain of information security: the purposeful blending of otherwise disjointed perspectives, goals, and methodologies in order to achieve a whole that is greater than the sum of its parts.

As one considers the critical information networks of the public and the private domains which enable and sustain the full range of societal activities within Maryland, educating current and future information security leaders on the concepts and techniques of purple teams and operations is a simple investment which will produce beneficial results far out of proportion to the effort. Given Maryland's leading national

1 The Rise of 'Purple Teaming,' Joseph R. Salazar, Dark Reading (6/13/2019), https://www.darkreading.com/threat-intelligence/the-rise-of-purple-teaming/a/d-id/1334909
2 http://gohs.maryland.gov/va/ and http://www.mcac.maryland.gov/how_to_help/H2H_CIP/index.html
3 http://gohs.maryland.gov/va_accomplishments/

role in the information security industry, it is only natural that the state should offer the first program of its kind which addresses this cutting edge trend and best practice.

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

Increase student success with less debt

This program will address the State Plan's goals to increase student success with less debt. Approximately 33% of our students fully fund their studies by way of employer tuition reimbursement, while another 43% utilize veteran education benefits. Currently, SANS Technology Institute does not participate in Title IV federal student loan programs and thus do not anticipate the creation of any student debt via this program. Similarly, our student retention and graduation rates for our graduate certificate students remains consistently stable at greater than 85%.

Support for veterans

The Purple Operations program also targets elements of other Strategies in the Maryland State Plan. Strategy 7 calls for special efforts to support veterans. Approximately 43% of our current study body is comprised of veterans, with nearly all of them using some combination of GI Bill benefits and employer tuition reimbursement to increase their knowledge and skills as they enter or further establish themselves in the civilian workforce. Given their inherent familiarity with joint operations and the integration of offensive and defensive activities, this program will draw upon the ingrained perspective of military veterans who are seeking to advance their information security careers.

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

1. 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 states that the supply of cybersecurity workers nationally is "very low," with 285,681 job openings relative to a total employed workforce of 746,858 (a ratio of 0.38, or, "for every 100 employed workers, the market seeks another 38 people"). The ratio of "openings requesting a GIAC certification" to "holders of GIAC certifications" is nearly twice as high at 0.64 (or, "for every 100 current GIAC certification holders, the market seeks another 64"). In Maryland alone, CyberSeek shows that there are 1,769 current job openings that specifically request GIAC certification holders. These data indicate a high demand not just for cybersecurity workers, but especially for those who have proven, by holding GIAC certifications, that they have the skills to do the job.

Table 1. Current Positions and Projected Growth to 2024 in CyberSeek's "Top Cybersecurity Job Titles"			
Job Title	**Maryland Positions in 2014**	**Growth to 2024**	**Growth in Percent**
Cyber Security Engineer			
Cyber Security Analyst	3,514	1,829	52%
Network Engineer/Architect	5,678	1,534	27%
Cyber Security Manager/Administrator	9,780	2,494	25%
Software Developer/Engineer	29,677	10,423	35%
Systems Engineer			
Systems Administrator	14,206	3,606	25%
Vulnerability Analyst/Penetration Tester			
IT Auditor	28,974	6,282	22%
Total	**91,829**	**26,168**	**28%**

Source: http://www.dllr.state.md.us/lmi/iandoproj/maryland.shtml (accessed April 2, 2020).

CyberSeek estimates the number of current cybersecurity job openings in Maryland at 14,535, which is not inconsistent with the DLLR numbers.

Sitting at the peak of all of this market demand and a workforce of tens of thousands is, logically, the emerging need for skilled technical leaders who understand both defensive, or blue, and offensive, or red, skills and mindsets.

2. Current and Projected Supply of Prospective Graduates

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

D. Reasonableness of Program Duplication

1. Similarities and Differences between the Purple Security Operations Program and Other Programs Awarding the Same Degree

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.

Currently, we are unaware of any educational program which is specifically seeking to produce technically educated leaders who are prepared to lead purple teams and operations. In order to contribute to further synergy and partnership across the public-private divide being bridged by the State's fusion center, educated leaders in the private sector with expertise in this domain will serve as force multipliers for Maryland's Core Goal #6. The STI Purple Security Operations graduate certificate program is intended to produce these leaders.

Our analysis of these factors clearly demonstrates that the STI Purple Security Operations program is not duplicative in any way, and that it is an important addition to the educational offering in Maryland. A scan was conducted of the MHEC "Classification of Instructional Programs" (CIP) database to check for similar existing programs at any MHEC authorized institution of higher education. Specifically, we looked at the following CIPs:

COMPUTER AND INFORMATION SCIENCES, GENERAL- 110101
INFORMATION TECHNOLOGY- 110103
INFORMATION SCIENCE/STUDIES- 110401
COMPUTER SYSTEMS NETWORKING AND TELECOMMUNICATIONS- 110901
COMPUTER AND INFORMATION SYSTEMS SECURITY- 111003

We detected no similar programs with this specific focus at any degree level.

Degree to Be Awarded

Graduate certificate.

Specific Academic Content of the Program; Evidence of Equivalent Competencies

No other institution currently enables students and graduates to earn industry-recognized certification exams as a core element of their program. Graduates of STI's Purple Security Operations program will hold at five industry-recognized GIAC certifications in addition to their graduate certificate, each of which is generally recognized by employers as a reliable indicator of professional skill.

Alternative Means of Educational Delivery, including Distance Education

STI's Purple Security Operations program has the unique ability to offer students the flexibility to take their courses either through live in-classroom instruction or via our award-winning OnDemand distance-learning system. The program also enables students

to enroll with an individualized, flexible academic plan that allows each of them to continue to work a full-time job while they complete the program.

3. Role and Mission

- Cybersecurity education is the sole focus of STI's mission**.** As discussed in section A.2., Relation to STI Mission and Strategic Goals, above, the alignment between our mission, vision, and goals and the specific purpose of this proposed graduate certificate program intersects exactly with Maryland Core Goal #6 by creating future leaders in both the public and private sectors who will work together to project Maryland's critical enterprise networks.

Admissions Requirements

STI's admission requirements for Purple Security Operations program will be as already established for our existing graduate certificate programs:

- Have at least 12 months of professional work experience in information technology, security or audit
- Be employed or have current access to an organizational environment that allows you to apply the concepts and hands-on technical skills learned in the program. This requirement may be waived under certain circumstances given the current situation and uncertainty about unemployment rates at specific times.
- Have earned a baccalaureate degree from a recognized college or university, or equivalent international education, with a minimum cumulative grade point average of 2.80

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

1. Discuss the Program's Potential Impact On High-Demand Programs at HBIs

No HBI offers a comparable credential.

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

1. Discuss the Program's Potential Impact on the Uniqueness, Identities of HBIs

Generally, the Purple Security Operations program has no impact on the uniqueness or identity of any of the HBIs.

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

1. Program Outline and Requirements

Required Courses

Required core courses (6 credit hours):

Students will take these two core courses:
ISE 6310 (SANS Course SEC 460): Enterprise Threat and Vulnerability Assessment | GEVA: GIAC Enterprise Vulnerability Assessor (3 credits)
ISE 6215 (SANS Course SEC 501): Advanced Security Essentials - Enterprise Defender | GCED: GIAC Certified Enterprise Defender (3 credits)

Capstone Course (3 credit hours)

ISE 6250 (SANS Course SEC 599): Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses | GDAT: GIAC Defending Advanced Threats (3 credits)

ISE 6310 Enterprise Threat and Vulnerability Assessment (3 credits)

SANS class: SEC 460, Enterprise Threat and Vulnerability Assessment
Assessment: GIAC GEVA
3 Credit Hours

ISE 6310, Enterprise Threat and Vulnerability Assessment, covers threat management, introduces the core components of comprehensive vulnerability assessment, and provides the hands-on instruction necessary to produce a vigorous defensive strategy

ISE 6310 teaches the use of industry-standard security tools for vulnerability assessment, management, and mitigation. The student will learn on a full-scale enterprise cyber range of target machines representative of an enterprise environment, leveraging production-ready tools and a proven testing methodology. This course also emphasizes a personnel-centric approach to security by examining the shortfalls of many vulnerability assessment programs in order to provide the student with the tactics and techniques required to secure networks against even the most advanced intrusions.

The course concludes with a discussion of triage, remediation, and reporting before putting the student's skills to the test on the final day against an enterprise-grade cyber range with numerous target systems to analyze and explore. The cyber range is a large environment of servers, end-users, and networking gear that represents many of the systems and topologies used by enterprises.

ISE 6215 Advanced Security Essentials – Enterprise Defender (3 credits)

SANS class: SEC 501 Advanced Security Essentials - Enterprise Defender
Assessment: GIAC GCED
3 Credit Hours

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

ISE 6250 Defeating Advanced Adversaries – Purple Team Tactics & Kill Chain Defenses (3 credits) (Capstone Course)

SANS class: SEC 599 Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses
Assessment: GIAC GDAT
3 Credit Hours

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

Electives Courses: (6 credit hours)

Students will select one elective from each category (Blue and Red).

Blue Electives (students will pick one):
ISE 5401 (SANS Course SEC 503): Intrusion Detection In-Depth | GCIA: GIAC Certified Intrusion Analyst (3 credits)
ISE 6240 (SANS Course SEC 511): Continuous Monitoring and Security Operations | GMON: GIAC Continuous Monitoring Certification (3 credits)

Red Electives (students will pick one):
ISE 6320 (SANS Course SEC 560): Network Penetration Testing and Ethical Hacking | GPEN: GIAC Penetration Tester (3 credits)
ISE 6360 (SANS Course SEC 660): Advanced Penetration Testing, Exploit Writing, and Ethical Hacking | GXPN: GIAC Exploit Researcher and Advanced Penetration Tester (3 credits)

ISE 5401 Intrusion Detection In-Depth (3 credits)

SANS class: SEC503: Intrusion Detection In-Depth
Assessment: GIAC GCIA
3 Credit Hours

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

ISE 6240 Continuous Monitoring and Security Operations (3 credits)

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

ISE 6320 Network Penetration Testing and Ethical Hacking (3 credits)

SANS class: SEC 560 Network Penetration Testing and Ethical Hacking
Assessment: GIAC GPEN
3 Credit Hours

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

ISE 6360 Advanced Penetration Testing, Exploits, and Ethical Hacking (3 credits)

SANS class: SEC 660 Advanced Penetration Testing, Exploits, and Ethical Hacking
Assessment: GIAC GXPN
3 Credit Hours

ISE 6360 builds upon ISE 6320 - Network Penetration Testing and Ethical Hacking. This advanced course introduces students to the most prominent and powerful attack vectors, allowing students to perform these attacks in a variety of hands-on scenarios.

2. Educational Objectives and Intended Student Learning Outcomes

The five primary educational objectives of the program are to:

a) PLO1: Practice and demonstrate mastery of fundamental network security knowledge and skills.
b) PLO2: Understand, practice, and demonstrate mastery of important defensive techniques and identify indications of an attack in order to detect / respond to/ mitigate incidents on enterprise networks.
c) PLO3: Understand, practice, and demonstrate mastery of important attacker techniques and be able to utilize the full range of penetration techniques in order to breach a network, pivot within it, and disrupt, exploit, or exfiltrate data from it.
d) PLO4: Utilize a broad range of both blue team and red team tools, technologies, and mindsets in the integrated design and implementation of purple security activities and exercises in order to maximize the synergy of full spectrum security operations.

The intended student learning outcomes are directly supported by the fulfillment of these core course learning objectives:

PLO 1: ISE 6310 Enterprise Threat and Vulnerability Assessment

- This core course provides an introduction to information security vulnerability assessment fundamentals, followed by in-depth coverage of the Vulnerability Assessment Framework. It then moves into the structural components of a dynamic and iterative information security program. Through a detailed, practical analysis of threat intelligence, modeling, and automation, students will learn the skills necessary to not only use the tools of the trade, but also to implement a transformational security vulnerability assessment program.

PLO 1: ISE 6215 Advanced Security Essentials – Enterprise Defender

- This core course teaches students how to build a comprehensive security program focused on preventing, detecting, and responding to attacks via the identification of the core components of building a defensible network infrastructure and an understanding of how to properly secure routers, switches, and network infrastructure. The course also instructs on the methods to detect advanced attacks on compromised systems, to include the formal methods for performing a penetration test to find weaknesses in an organization's security apparatus. The course concludes by teaching how to respond to an incident using the six-step process of incident response (Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned), as well as approaches to analyzing malware, ranging from fully automated analysis to static properties analysis, behavioral analysis, and code analysis.

PLO 2: ISE 5401 Intrusion Detection In-Depth

- This course delivers the technical knowledge, insight, and hands-on training which students need to defend their network 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. Students will get plenty of practice learning to master a variety of tools, including tcpdump, Wireshark, Snort, Zeek, tshark, and SiLK. Daily hands-on exercises suitable

for all experience levels reinforce the course book material so that students can transfer knowledge to execution. Bootcamp sessions and exercises force students to take the theory taught during the course and apply it to real-world problems immediately. Basic exercises include assistive hints, while advanced options provide a more challenging experience for students who may already know the material or who have quickly mastered new material.

Or,

PLO 2: ISE 6240 Continuous Monitoring and Security Operations

- No network is impenetrable, a reality that business executives and security professionals alike have had to accept. Prevention is crucial, and we can't lose sight of it as the primary goal. However, a new proactive approach to security is needed to enhance the capabilities of organizations to detect threats that will inevitably slip through their defenses. ISE 6240, Continuous Monitoring and Security Operations, teaches students how 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 best position an organization or Security Operations Center (SOC) to analyze threats and detect anomalies that could indicate cybercriminal behavior. The National Institute of Standards and Technology (NIST) developed guidelines described in NIST SP 800-137 for Continuous Monitoring (CM), and day five of this course teaches students how to implement CM using the NIST framework.

PLO 3: ISE 6320 Network Penetration Testing and Ethical Hacking

- With comprehensive coverage of tools, techniques, and methodologies for network penetration testing, ISE 6320 prepares students to conduct high-value penetration testing projects. The course starts with proper planning, scoping and recon, then covers scanning, target exploitation, password attacks, web app manipulation, and attacking the Windows domain, with over 30 detailed hands-on labs throughout. Students learn how to perform detailed reconnaissance, studying a target's infrastructure by mining blogs, search engines, social networking sites, and other Internet and intranet infrastructures. Hands-on labs equip students to scan target networks using best-of-breed tools. After scanning, students learn dozens of methods for exploiting target systems to gain access and measure real business risk, to include post-exploitation, password attacks, and web apps, and pivoting through the target environment to model the attacks of real-world bad guys to emphasize the importance of defense in depth. Finally, this course focuses on the technological heart of most organizations, the Windows Domain, to include the technical details of Kerberos and Active Directory.

Or,

PLO 3: ISE 6360 Advanced Penetration Testing, Exploit Writing, and Ethical Hacking

- ISE 6360 is designed as a logical progression point for those who have previously completed ISE 6320, or for those with existing penetration testing experience. Students

with the prerequisite knowledge to take this course will walk through dozens of real-world attacks used by the most seasoned penetration testers. The methodology of a given attack is discussed, followed by exercises in a hands-on lab to consolidate advanced concepts and facilitate the immediate application of techniques in the workplace. Each day of the course includes a two-hour boot camp to drive home additional mastery of the techniques discussed. A sample of topics covered includes weaponizing Python for penetration testers, attacks against network access control (NAC) and virtual local area network (VLAN) manipulation, network device exploitation, breaking out of Linux and Windows restricted environments, IPv6, Linux privilege escalation and exploit-writing, testing cryptographic implementations, fuzzing, defeating modern OS controls such as address space layout randomization (ASLR) and data execution prevention (DEP), return-oriented programming (ROP), and Windows exploit-writing.

PLO 4: ISE 6250 Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses

- ISE 6250, the capstone course for this program, arms students with the knowledge and expertise needed to overcome today's threats. Recognizing that a prevent-only strategy is not sufficient, this course introduces security controls aimed at stopping, detecting, and responding to adversaries. ISE 6250 gives students real-world examples of how to prevent attacks by way of more than 20 labs plus a full-day Defend-the-Flag exercise during which students attempt to defend a virtual organization from different waves of attacks against its environment. This six-part course starts off with an analysis of recent attacks through in-depth case studies, explaining what types of attacks are occurring and introducing formal descriptions of adversary behavior such as the Cyber Kill Chain and the MITRE ATT&CK framework. In order to understand how attacks work, students will also compromise a virtual organization in section one exercises. In sections two, three, four and five, this course teaches how effective security controls can be implemented to prevent, detect, and respond to cyber attacks. The topics to be addressed include:

    - Leveraging MITRE ATT&CK as a "common language" in the organization
    - Building a Cuckoo sandbox solution to analyze payloads
    - Developing effective group policies to improve script execution (including PowerShell, Windows Script Host, VBA, HTA, etc.)
    - Highlighting key bypass strategies for script controls (Unmanaged Powershell, AMSI bypasses, etc.)
    - Stopping 0-day exploits using ExploitGuard and application whitelisting
    - Highlighting key bypass strategies in application whitelisting (focus on AppLocker)
    - Detecting and preventing malware persistence
    - Leveraging the Elastic stack as a central log analysis solution
    - Detecting and preventing lateral movement through Sysmon, Windows event monitoring, and group policies
    - Blocking and detecting command and control through network traffic analysis
    - Leveraging threat intelligence to improve security posture

- During the Defend-the-Flag challenge in the final course section, students will be pitted against advanced adversaries in an attempt to keep a network secure.

Each program learning outcome and course objective listed above is measured by the respective GIAC certification examination associated with each of the five courses that the student completes from those listed in Section G1.

Learning objectives are updated at least every four years after the assessment of rigorous, detailed, and updated job task analyses that have made the passing of these exams globally recognized as being indicative of having mastered the knowledge taught in our technical courses and the capabilities required to engage in real-world cybersecurity activities.

3. How General Education Requirements Will Be Met

As an graduate certificate program, the Purple Security Operations does not include general education requirements.

4. Specialized Accreditation/Certification Requirements

Each student who earns a Purple Security Operations graduate certificate will have achieved certification in five areas of cybersecurity using Global Information Assurance Certifications (GIAC).

H. Articulation

As a technically focused graduate certificate program and the first of its type, no articulation agreements are anticipated.

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

The faculty serving the students of the proposed Purple Security Operations program is comprised of the very same instructors who currently teach the 1000+ enrolled graduate and undergraduate students at the SANS Technology Institute as well as the more than 30,000 professionals across the globe each year enrolled at SANS via live and online courses. Their qualifications to fulfill our mission were recently reviewed and confirmed by the Visiting Team of the Middle States Commission on Higher Education as part of STI's re-accreditation review in 2018.

Adding 25 to 50 students (see Section L, Financial Resources) to the instructors' teaching load is the equivalent of far less than 1% increase in enrollment per class. Therefore, we conclude that our faculty is more than adequate in both capability and number to serve this new program.

Meeting STI's mission requires that STI faculty and graduates are "scholar-practitioners." STI uses the term "scholar-practitioner" to designate people who are both (1) highly trained professional practitioners focused on information security, and (2) scholars in the sense that they both contribute to and consume the research required to advance that professional practice. The combination enables them to incorporate new

research into their work and create the new knowledge and solutions that others seek to use. Our faculty are not solely scholars, they must also be advanced practitioners of the subjects they teach so that they can show STI students how to practice security effectively. This gives STI students an advantage relative to graduates of other programs in which students learn theory, but not up-to-date practice. Finally, our faculty must be talented teachers, able to communicate often-difficult technical information in a clear and compelling manner.

Among STI's faculty are people who are called upon to investigate attacks on the U.S. government and our largest commercial enterprises, who are entrusted to teach practitioners of cybersecurity at the highest and most sensitive (classified) levels, and who, through their professional practice and research, advance our understanding of cyber threats and potential remediation and then transmit that knowledge forward to our students and the larger community. Even beyond their superlative technical abilities, our faculty have skills as teachers that truly set them apart and allow them to impart sometimes dense technical lessons with enthusiasm, applicable real-world examples, and charismatic engagement.

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

- President Alan Paller was the Co-chair of the Department of Homeland Security's Task Force on CyberSkills, and had been a Charter Member of President Clinton's National Information Assurance Council.
- President Paller, Dr. Eric Cole, and James Lyne are three of fewer than 30 people currently listed on the Infosecurity Europe Hall of Fame.
- Dr. Johannes Ullrich was recognized as one of the 50 most powerful people in networking by NetworkWorld. Social media is replete with examples of references to SANS Instructors, including items like Security Leaders to Follow on Social Media.
- STI faculty are repeatedly invited to keynote presence at RSA, the industry's largest convocation for information security research and practice. For each of the last seven years, members of STI's faculty, led by President Alan Paller, have hosted one of the main keynotes at "RSA," focusing their presentation on their expectations for the seven most dangerous new attack techniques they expect to impact the industry in the subsequent year. The press release regarding the entire event issued by RSA is indicative of our faculty's prominence in the industry: not only are they one of the three keynotes highlighted (together with a Cryptographer's panel, which is the core activity of RSA), but they are presented prior to and in advance of the CEOs, Presidents, and leading executives from companies such as Microsoft, Hewlett Packard Enterprise, Symantec, Intel Security, and Cisco Security.
- STI faculty are sought after by the news media for their commentary on cybersecurity topics – STI faculty are frequently sought-after as commentators for breaking news articles on adverse cyber events. Their commentary appears in general news publications such as the New York Times and Wall Street Journal, in general magazines such as Forbes and Fortune, and their work is highlighted on various TV news programs. They are sought-after speakers even for general industry events, such as TED (James Lyne's February, 2013 TED talk on 'everyday cybercrime' has been viewed nearly 1.7 million times).

As shown in Figure 1 (below), the SANS instructor development and assessment process requires a prospective STI faculty member to successfully complete four increasingly competitive steps (listed here and described in greater detail below):
(1) Earn scores on a Global Information Assurance Certification (GIAC) examination above 85.
(2) Earn high marks in mentoring (lab/teaching assistant) two groups of students.
(3) Earn high marks as "community instructors" in teaching two classes held at small Residential Institutes.
(4) Earn high marks as a supervised instructor at a large Residential Institute.

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

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

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

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

Figure 1 SANS Instructor Development and Assessment Process

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

Once appointed, qualified individuals serve in dual roles as SANS Instructors and STI faculty members. Each appointed instructor is a proven, real-world practitioner whose

experiences are especially relevant to the school, enabling them to author courses of value, relevancy, and currency, as well as to deliver these courses to students in an effective, highly engaging manner that includes supplying ever-renewed examples from their work practice. These industry-recognized demarcations indicate technical achievement in the field, superior teaching effectiveness and student engagement as exemplified in the classroom and online, and successful completion of a competitive development process that employs both student and peer-faculty feedback to prove that the instructors possess these qualities.

While a handful of faculty members serve in full-time teaching and research roles, most are adjunct, scholar-practitioners who teach less than full-time for the school or our parent, SANS, so that they can engage in the practice of cybersecurity, keep their skills advanced and current, and feed their experiences and learnings back into the courses and class discussions.

STI's current faculty leadership, especially as it pertains to the proposed Purple Security Operations graduate certificate program, includes the following individuals:

Stephen Sims (ISE 6215, ISE 6250, ISE 6360)

Stephen became a SANS instructor in 2006, and today is curriculum lead for SANS Penetration Testing and SANS Cyber Defense curricula, and is a faculty fellow for the SANS Institute. He authored SANS' only 700-level course, SEC760: Advanced Exploit Development for Penetration Testers, which concentrates on complex heap overflows, patch diffing, and client-side exploits. He's the lead author of SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking, as well as the co-author of SEC 599 Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses, this program's capstone course. He also routinely teaches SEC501: Advanced Security Essentials - Enterprise Defender.

Stephen is the 9th person in the world to receive the prestigious GIAC Security Expert certification (GSE). He is a Certified Information Systems Auditor (CISA) and certified Immunity Network Offense Professional (Immunity NOP), along with many other certifications.

An author of the Gray Hat Hacking book series, Stephen holds a master's degree in information assurance from Norwich University. A frequent presenter, Stephen has spoken at RSA USA for the past five years and was keynote speaker for the 2019 event. He's also presented at OWASP AppSec, BSidesCharm, AISA, and more.

Matthew Toussain (ISE 6310, ISE 6320)

Since graduating from the U.S. Air Force Academy in 2012 with a B.S. in computer science, Matthew Toussain has served as the senior cyber tactics development lead for the U.S. Air Force (USAF) and worked as a security analyst for Black Hills Information Security. In 2014, he started Open Security, which performs full-spectrum vulnerability risk assessments.

Matthew teaches SEC460: Enterprise Threat and Vulnerability Assessment and SEC560: Network Penetration Testing and Ethical Hacking. He worked with other SANS instructors to develop SEC460, Enterprise Threat and Vulnerability Assessment. In addition to teaching at SANS, he is an avid supporter of cyber competitions and participates as a red team member or mentor for the Collegiate Cyber Defense Competition (CCDC), the annual NSA-led event Cybersecurity Defense Exercise (CDX), and SANS Institute"s NetWars.

In addition to his BS in Computer Science, Matthew is a graduate of STI's Master of Science in Information Security Engineering program.

David Hoelzer (ISE 5401)

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

Eric Conrad (ISE 6240)

SANS Faculty Fellow Eric Conrad is the lead author of SANS MGT414: SANS Training Program for CISSP® Certification, and coauthor of both SANS SEC511: Continuous Monitoring and Security Operations and SANS SEC542: Web App Penetration Testing and Ethical Hacking. He is also the lead author of the books the CISSP Study Guide, and the Eleventh Hour CISSP: Study Guide.

Eric's career began in 1991 as a UNIX systems administrator for a small oceanographic

communications company. He gained information security experience in a variety of industries, including research, education, power, Internet, and health care. He is now CTO of Backshore Communications, a company focusing on hunt teaming, intrusion detection, incident handling, and penetration testing. He is a graduate of the SANS Technology Institute with a master of science degree in information security engineering. In addition to the CISSP, he holds the prestigious GIAC Security Expert (GSE) certification as well as the GIAC GPEN, GCIH, GCIA, GCFA, GAWN, and GSEC certifications.

Tim Medin (ISE 6320)

Tim began his security career in 2008 with a role at AgStar Financial Services (now Compeer Financial), and since then has worked for FishNet Security (now Optiv) and Counter Hack. Today, he's the founder and principal consultant at Red Siege.

A SANS instructor since 2012, Tim is currently the program director for the SANS Master of Science in Information Security Engineering (MSISE) curriculum, as well as a principal instructor and course author. He teaches both SEC560: Network Penetration Testing and Ethical Hacking and SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking.

Through the course of his career, Tim's had the opportunity to hack some of the best and biggest companies on earth and get a sneak peek inside cutting-edge technology before it's publicly released. He has performed penetration tests on a wide range of organizations and technologies in industries including control systems, higher education, financial services, and manufacturing, and brings years of practical experience to his STI students. Tim is an experienced international speaker and the creator of Kerberoasting, a widely-used technique to extract kerberos tickets in order to offline attack the password of enterprise service accounts. He has an MBA from the University of Texas, holds the GWAPT, GPEN, GMOB, GCED, and GCIH certifications, and previously held the CCNA certification.

A summary list of these Purple Security Operations graduate certificate faculty is available in Appendix 3.

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

Ongoing Pedagogy Training for Faculty:

Instructional pedagogy is an ingrained element of the SANS instructor developmental program, from which STI draws its faculty, and is reinforced during live teaching engagements and routinely during Curriculum Lead meetings. This instructional process is then continued on a recurring basis for new and current faculty members.

The SANS development and continuous assessment process ensures that persons eventually chosen to teach STI students demonstrate (1) mastery in the community of practice in which they instruct, and (2) highly rated and effective teaching practices. An equally important element of teaching quality at STI is that SANS' ongoing assessment

processes enable the college to ensure that teaching faculty retain both a high degree of technical mastery and outstanding teaching skills on an ongoing basis.

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

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

These reports not only demonstrate the ongoing, continual assessments performed by faculty leadership, to include the Curriculum Leads (more below on this position), they further provide timely and recurring opportunities to reinforce best practices and institutional pedagogy. While these data are distributed and reviewed each day, analysis of the quarterly summaries and comparison reports generates recognition of longer-term issues, opportunities for further faculty development, and required corrective actions. Curriculum Leads, who act as the equivalent of "Department Heads" both for SANS and STI, play an important role in the management and development of other faculty. They are thought leaders individually, but they are also charged with the oversight of all courses within their curriculum, and meet as a group twice per year to review their curricula and pedagogy with each other. Individual faculty with identified performance issues, as highlighted on these quality assessment reports, are engaged by Curriculum Leads for further investigation and instruction.

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

LMS and Distance Education Training for Faculty:

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

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

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

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

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

J. Adequacy of Library Resources (outlined in COMAR 13B.02.03.12).

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

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

with access to raw data, summaries, and query facilities to analyze malicious Internet traffic records. This is a rich data source for advanced security research projects that analyze attack patterns and how fast worms and other attacks spread through the Internet.

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

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

This program will be offered in combinations of various online modalities and, in normal times, at residential institutes. More than 400 residential institutes are routinely available, under normal travel conditions, to Purple Security Operations students each year with a cumulative capacity of more than 40,000 students.

Additionally, the Purple Security Operations program draws on SANS's online technology that currently serves more than 18,000 students each year which is not capacity-constrained and is available globally and around-the-clock.

Finally, building upon our ten years of experience at delivering synchronous and asynchronous online education, we have improved and expanded our online delivery capabilities to include our new "Live Online" format, which essentially replicates a residential learning experience via a 1-, 2-, 3-, or 6-week format. Thus, the proposed program will easily be accommodated in the existing in-person training programs. Currently scheduled live courses described in this curriculum can be found online here.

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

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

Table 1:
RESOURCES

Resource Categories	Year 1	Year 2	Year 3	Year 4	Year 5
1. Reallocated Funds	0	0	0	0	0
2. Tuition/Fee Revenue (c + g below)	210000	480000	435000	472500	622500
a. Number of F/T Students	20	32	33	37	37
b. Annual Tuition/Fee Rate	10500	10500	10500	10500	10500
c. Total F/T Revenue (a x b)	225000	367500	367500	388500	388500
d. Number of P/T Students	0	0	0	0	0
e. Credit Hour Rate	0	0	0	0	0
f. Annual Credit Hour Rate	6	6	6	6	6
g. Total P/T Revenue (d x e x f)	0	0	0	0	0
3. Grants, Contracts & Other External Sources	0	0	0	0	0
4. Other Sources	0	0	0	0	0
TOTAL (Add 1 – 4)	225000	367500	367500	388500	388500

Table 2:
EXPENDITURES

Expenditure Categories	Year 1	Year 2	Year 3	Year 4	Year 5
1. Faculty (b + c below)	11250	24000	21750	23625	31125
a. # Sections offered	N/A	N/A	N/A	N/A	N/A
b. Total Salary	6750	14400	13050	14175	18675
c. Total Benefits	4500	9600	8700	9450	12450
2. Admin. Staff (b + c below)	16800	42000	42000	42000	58800
a. # FTE	0.2	0.5	0.5	0.5	0.7
b. Total Salary	12000	30000	30000	30000	42000
c. Total Benefits	4800	12000	12000	12000	16800
3. Support Staff (b + c below)	0	0	0	0	0
a. # FTE	0	0	0	0	0
b. Total Salary	0	0	0	0	0
c. Total Benefits	0	0	0	0	0
4. Equipment	0	0	0	0	0
5. Library	0	0	0	0	0
6. New or Renovated Space	0	0	0	0	0
7. Other Expenses	90000	147000	147000	155400	155400
TOTAL (Add 1 – 7)	118050	213000	210750	221025	245325

Finance Data: Narrative

Table 1: RESOURCES

1. Re-allocated Funds
   Narrative: Analyze the overall impact that the reallocation will have on the institution, particularly on existing programs and organizations units.
   N/A

2. Tuition and Fee Revenue
   Narrative: Describe the rationale for the enrollment projections used to calculate tuition and fee revenue.
   STI is currently recruiting 20-30 new graduate certificate students per month, with approximately one-third typically going into our Penetration Testing program, one-third into our Incident Response program, and the remaining one-third split into the Cyber Defense, Cyber Core, and Industrial Control systems programs. Thus, it is our more narrowly-focused graduate certificate programs which attract the greatest number of new students; however it is also true that penetration testing and incident response are required functions across many

industries. We believe that market and industry pressures will similarly elevate the attractiveness of this advanced, multi-faceted graduate certificate program to eventually be nearly on par with our two largest certificate programs.

The tuition projection for Year 1 assumes the Purple Security Operations program admits 20 full-time students during the course of the year, each of whom pay $5,250 per course. Currently, our graduate students complete an average of 2 courses per year, supporting an effective annual tuition of $10,500 per year per student.

In Year 2, we assume that the rate of admission to the program will drop slightly, after attracting a "backload" of prospective students, to admit 15 new students. As most of our graduate certificate students take roughly two years to complete their programs, this second year of growth is purely additive. Also, the two-year retention rate for graduate certificate students is approximately 85%. This retention rate is factored into the prior year's admitted number, and is added to the current year's admitted number to combine to a total number of students for that given year. Thus, the net total number students in year 2 is effectively 32.

For years 3, 4, and 5 we project 20 new students per year. Applying the same logic presented above, this leads to a total effective student counts of 33, 37, and 37, respectively. We believe expectations for this growth are reasonable because we will be able to expand the offering of the program to students from other states via our online modalities.

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

4. Other Sources
   Narrative: Provide detailed information on the sources of the funding, including supporting documentation. N/A

5. Total Year
   *Narrative: Additional explanation or comments as needed.*N/A

Table 2: EXPENDITURES

Faculty
Purple Security Operations 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, and the Purple Security Operations 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, Purple Security Operations 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 Purple Security Operations students, either live or online. In addition, 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, at an effective rate of 5% of tuition revenue. Thus, for the sake of clarity, we have estimated a proportional cost for faculty salary and benefits as a percentage of total course load increase which is expected due to the creation of this new graduate certificate program.

Administrative and Support Staff
The STI graduate programs currently operate at a ratio of students to administrative staff ratio of 150:1 in cases where a student advisor's workload consists entirely of graduate certificate students (as compared to those advisors who also, or only, work with master's students). Average salary and benefit information is reflective of our current cost experience and market expectations.

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

Other Expenses
As described elsewhere, a core design element of the SANS Technology Institute 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 Purple Security Operations program will also benefit from this financial arrangement. The financial projections assume the same mix of payments that STI incurs today per student, as recently reviewed by the Middle States evaluation team during our re-accreditation study.

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

Continuous, closed-loop evaluation has been the hallmark of STI programs since the 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 Purple Security Operations 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 graduate certificate program undergoes a formal review by an evaluation team comprised of subject matter experts every four years. This review process will ensure alignment of (1) course outcomes to program learning objectives, of (2) program learning objectives to any capstone requirements, and of (3) both program learning objectives and capstone requirements to a survey of industry requirements.

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

TBD

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

Not applicable.

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

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

Appendix 1. Contracts with Related Entities

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

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

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

- **STI's programs designed by STI faculty** – STI's academic programs were designed by the faculty in order to optimally achieve their stated learning outcomes. For each program, the faculty responsible for program design built out the educational content from three distinct sources:
    - **SANS Technical and Management Courses** – SANS maintains the world's largest and most-respected catalog of 36-50 seat-hour courses in cybersecurity, ranging from broad survey courses in cyber defense to highly advanced and specialized penetration testing and digital forensics courses. Each program includes a subset of SANS courses relevant to achieving that program's learning

outcomes, including the availability of elective courses. In addition, STI students may avail themselves of all the opportunities at different times and locations throughout the United States (and world) that the courses are offered live and taught by STI faculty, or they may also take the opportunity to take the very same course presented online by SANS, which transforms the best live performance by an STI faculty member into the online version of the course, complete with the same labs and access to subject-matter experts online. STI thereby offers an extraordinarily broad set of choices for students to tailor their program schedule to fit within their work and personal lives.

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

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

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

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

Purpose

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

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

Vision

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

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

Mission

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

Scope

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

Hours of Operations

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

Service Expectations

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

Accounting and Finance

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

Bursar & Registration

Process	Service Expectation	Service Metric

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

Human Resources

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

Marketing

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

Information Technology

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

Technical Course Maintenance & Presentation

Process	Service Expectation	Service Metric
Currency of content	Make available for use by STI Faculty any and all technical content developed by the SANS Institute	Content is reviewed at least semi-annually for currency with existing malicious capabilities and mitigation theory and strategy

Quality of content and presentations	Assist through all means necessary and available the delivery of STI faculty and lab instruction in a high-quality fashion	SANS Institute will make available all performance ratings derived from students on STI courses or faculty

Educational Residency

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

Service Constraints

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

Terms of Agreement

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

Periodic Quality Reviews

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

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

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

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

Service Level Maintenance

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

Issue Resolution

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

Payment Terms and Conditions

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

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

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

Date: Date:

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

STI Course	SANS Course	Payment Amount
ISE 5101	SEC 401	$1,500
ISM 5101	MGT 512	$1,500
ISE/M 5201	SEC 504	$1,500
ISE/M 5300	MGT 433	$ 500
ISM 5400	MGT 514	$1,500
ISE 5401	SEC 503	$1,500
ISE/M 5500	N/A	$ 0
ISE 5600	MGT 514 (Day 4)	$ 500
ISM 5601	LEG 523	$,1500
ISE/M 5700	N/A	$ 0
ISE/M 5800	MGT 525	$1,500
ISE/M 5900	N/A	$ 0
ISE/M 6001	SEC 566	$1,500
ISE/M 6100	N/A	$ 0
ISM 6201	AUD 507	$1,500
ISE/M 6215	SEC 501	$1,500
ISE 6230	SEC 505	$1,500
ISE 6235	SEC 506	$1,500
ISE 6240	SEC 511	$1,500
ISE/M 6300	NetWars Cont	$ 0
ISE 6315	SEC 542	$1,500
ISE 6320	SEC 560	$1,500
ISE 6325	SEC 575	$1,500
ISE 6330	SEC 617	$1,500
ISE 6350	SEC 573	$1,500
ISE 6360	SEC 660	$1,500
ISE 6400	DFIR NetWars Cont	$ 0
ISE 6420	FOR 500	$1,500
ISE 6425	FOR 508	$1,500
ISE 6440	FOR 572	$1,500
ISE 6450	FOR 585	$1,500
ISE 6460	FOR 610	$1,500
ISE 6515	ICS 410	$1,500
ISE 6520	ICS 515	$1,500
ISE 6615	DEV 522	$1,500
ISE 6715	AUD 507	$1,500
ISE 6720	LEG 523	$1,500
RES 5500	N/A	$ 0

RES 5900	N/A	$ 0

SANS Technology Institute-GIAC Memorandum of Understanding

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

Contents

Purpose

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

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

Vision

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

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

Mission

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

Scope

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

Hours of Operations

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

Service Expectations

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

Service Constraints

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

Terms of Agreement

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

Periodic Quality Reviews

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

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

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

STI's Executive Director and the Director of GIAC will meet annually.

Service Level Maintenance

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

Issue Resolution

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

Payment Terms and Conditions

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

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

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

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

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

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

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

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

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

(a) Curriculum and instruction

(i) A distance education program shall be established and overseen by qualified faculty.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

STI faculty members design all distance learning programs.

(b) Role and mission

(i) A distance education program shall be consistent with the institution's mission.

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

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

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

(c) Faculty support

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

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

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

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

Instructor Guidelines for SANS Simulcast Classes

What to Expect

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

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

Advance Planning

1. The vLive! and OnSite teams will schedule a planning call with the customer point of contacts two weeks before the course; please plan on attending this call.
2. The AV kit that contains all necessary equipment for the Simulcast will be shipped to the Simulcast location prior to class.

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

Audio Tips

6. Do not wear your cell phone on your belt next to the transmitter or lay it next to the receiver by the laptop. Your cell phone and student cell phones can create interference. You may need to disable Bluetooth functionality on your phone if it is causing buzzing.
7. Leave your wireless microphone on at all times, but turn off your GoToTraining audio during breaks. To do this, simply ask your on-site moderator to mute you on the Simulcast laptop.
8. ALWAYS repeat comments and questions from students at your location; remote students can hear you, but all other sound will be muffled or inaudible.

Starting Class

9. When it is time to start class, your moderator will start the recording and give you a signal that everything is ready on the remote side.
10. After the moderator has turned the class over to you, introduce yourself and briefly explain to students how the Simulcast class will work.
11. It is important to make the remote and on-site students aware of each other. Identify and welcome each remote site by name. A roster with the remote sites and student counts will be provided to you.
12. Please encourage remote students to participate by typing their questions and comments into the Chat window.
13. Directing questions about class material to the virtual students can also help to keep them engaged throughout the class.
14. The moderator will relay any questions from the online students to you.
15. Discuss any other housekeeping items as needed (timing of breaks, confirming that VMWare is correctly set up, etc.).

Teaching Tips

16. ALWAYS repeat comments and questions from students at your location; remote students can hear you, but all other sound will be muffled or inaudible.
17. If you need to discuss issues that students should not see, please use the “Organizers Only” or “private message” chat option as your means of communication.
18. Address remote students often to ensure they feel like they are part of the class; remote students become passive listeners if they are not actively engaged.
19. All scripts, videos, demos, etc. that you wish to show to students must be shared with GoToTraining’s application sharing feature.
20. Remote students’ systems (and your host’s network) can be slowed down if you send very large files. If a file is necessary for class try to send it before class or during a break. If it is not course-related (e.g., music while on break), consider not sending it.
21. Use the GoToTraining timer when breaking from lecture so remote students know when class will be resuming; tell the moderator how many minutes you would like and they will set up the timer for you.

22. When breaking for lunch, please explain to students that they will need to log out of the morning session and log into the afternoon session upon their return.
23. Allow plenty of time to log into GoToTraining when arriving in the morning or returning from lunch. Depending on the location, you may have to extend the lunch break.
24. Conduct a quick audio check after each break and lunch to confirm that your microphone is on and that your remote students can hear you.

Suggested Best Practices

Jason Fossen:

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

Jason Lam:

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

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

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

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

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

- The SANS Information Security Reading Room contains more than 2,000 original research studies, not available from any other source, in 76 knowledge domains relevant to the study of information security. They are downloaded more than a

million times each year. The Reading Room is available at http://www.sans.org/reading_room/.

- The SANS Security Policy Collection contains model security policies developed by major corporations and government agencies. The collection contains about 35 policies and grows as new security issues arise and policy templates are needed.
- The SANS Top-20 V7 is a consensus list of vulnerabilities that require immediate remediation. It is the result of a process that brought together dozens of leading security experts.
- The SANS Newsletter Collection helps keep students up to date with the high-level perspective of the latest security news.
- The Security Glossary is among the largest glossaries of security terms available on the Internet. It was developed jointly by SANS and the National Security Agency and provides authoritative definitions of many of the specialized terms students will encounter.
- The SANS Collection of Frequently Asked Questions about Intrusion Detection contains 118 authoritative discussions of the primary topics that arise when planning and implementing intrusion detection technologies. The collection is available at http://www.sans.org/security-resources/idfaq/.
- The SANS Internet Storm Center Archives contain contemporaneous analyses of new attacks that are discovered on the Internet. The archives constitute an extraordinary research asset because of the depth of the analysis and the currency of the topics covered. They also provide SANS students with access to raw data, summaries, and query facilities to analyze malicious Internet traffic records. This is a rich data source for advanced security research projects that analyze attack patterns and how fast worms spread through the Internet.
- SANS Web Briefings held several times a month feature SANS faculty and other security experts providing up-to-date web briefings for SANS alumni on new threats seen at the Internet Storm Center, new technologies that are emerging, and analysis of security trends.

(e) Students and student services

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

- Curriculum information is posted, in detail, at the SANS.EDU website at https://www.sans.edu/academics/

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

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

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

- Technical equipment requirements are posted with individual courses at the SANS course website.

- Learning management systems information is posted in detail at https://www.sans.org/ondemand/faq

- The availability of academic support services and financial aid resources is posted at https://www.sans.edu/students/services, and on page 33 of the Student Handbook at page 33, https://www.sans.edu/downloads/sti-student-handbook.pdf

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

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

With STI students taking approximately half of their credits through distance learning, the overall satisfaction with student services may be considered a reliable surrogate for effectiveness of distance learning student services. Evidence from student surveys indicates that measures of overall student satisfaction are high (above 90%)/. Quantified measures of specific sub-processes with student management were also high, with about 90% of respondents saying they were "Somewhat Satisfied" and "Very Satisfied" for each of the operational elements (Table A.4.2).

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

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

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

Our Purple Security Operations students will be experienced and working adult professionals in a highly technical field. Thus, they have the needed background, knowledge, and technical skills to use the distance learning modalities.

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

Advertising, recruiting, and admissions materials for Purple Security Operations students are currently being drafted. STI has a solid record of meeting Middle States' high standards for transparency and accuracy in all its marketing and admissions materials and will continue to do so.

(f) Commitment to support

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

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

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

STI has adequate faculty, infrastructure, and financial resources, as demonstrated in Sections H, J, and K, to implement the new Purple Security Operations program. Further, because the undergraduate program is core to our mission, and was specifically discussed during the Middle States 2018 Team Visit as a critical step for meeting that mission, we have demonstrated both the commitment and resources to maintain the program for many years.

(g) Evaluation and assessment

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

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

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

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

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

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

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

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

We will continue to monitor GIAC scores in the Purple Security Operations program, by delivery modality.

Appendix 3. Summary Listing of Purple Security Operations Graduate Certificate Faculty

Last Name	First Name	Highest Degree	Highest Degree Field	Academic Rank	Title	Status	Courses Taught
Sims	Stephen	Master's	Information Assurance	Faculty Fellow	Program Director (Purple Operations)	Full Time	ISE 6215, ISE 6250, ISE 6360
Toussain	Matthew	Master's	Information Security Engineering	Instructor	Instructor	Full Time	ISE 6310, ISE 6320
Hoelzer	David	Master's	Computer Science	Faculty Fellow	Dean of Faculty	Full Time	ISE 5401
Conrad	Eric	Master's	Information Security Engineering	Faculty Fellow	Professor	Full Time	ISE 6240
Medin	Tim	MBA	Business	Principal Instructor	Program Director (MSISE)	Full Time	ISE 6320

Memorandum of Understanding (MOU)
between
SANS Technology Institute (STI)
and
Montgomery College (MC)

I. IDENTIFICATION OF PARTIES

SANS Technology Institute (STI) is a cybersecurity undergraduate and masters-level college licensed by The Maryland Higher Education Commission (MHEC)_and accredited by the Middle States Commission on Higher Education, located at 11200 Rockville Pike, Rockville MD 20852.

Montgomery College (MC) is a public, open admissions community college located at 20200 Observation Drive, Germantown, MD 20876. MC has three campuses plus workforce development/continuing education centers and off-site programs throughout Montgomery County.

II. PREAMBLE

This MOU constitutes an agreement between STI and MC to facilitate the launch of STI's Bachelor of Professional Studies in Applied Cybersecurity (BACS) program. STI and MC have been partners in offering academic cybersecurity programs for nearly four years and worked together to design the BACS program.

We believe BACS will serve as a national model for a cost-effective academic pipeline that supplies highly skilled cybersecurity professionals qualified for elite positions with employers in Maryland and across the nation. Graduates of the BACS program will have completed all requirements for a bachelor's degree and in the process will complete seven advanced immersion cybersecurity courses and associated Global Information Assurance Certifications (GIAC) certifications. These same courses and certifications have been completed by more than 100,000 cybersecurity professionals, but their employers paid the costs. BACS graduates, on the other hand, will have completed those immersion courses and passed the challenging certification exams before entering the workforce. Thus, employers of BACS graduates will get new employees ready to perform at high levels without requiring months of additional advanced training and tens of thousands of dollars of additional training investment. For the graduates, the BACS will provide credentials that demonstrate hands-on cybersecurity skills and knowledge far beyond those offered in most graduate

cybersecurity degree programs, thereby saving the students years of extra study and tens of thousands of dollars in extra tuition.

With STI providing the upper division courses and Montgomery College providing the general education and foundational computer science and computer security courses, the BACS program is affordable and accessible for students throughout Montgomery County. In particular, the BACS will provide talented MC students with a direct pathway to qualify for cybersecurity jobs by earning multiple, highly valued, specialized cybersecurity certifications that are an integral part of completing the BACS degree. We intend for the BACS to be accessible to students throughout Maryland as additional Maryland community colleges decide to participate in the program by establishing articulation roadmaps like that shown in Table 1 below.

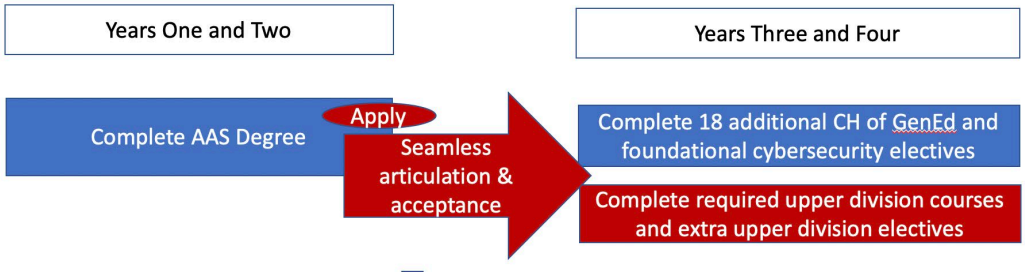
III. PATHWAYS TO A BACS DEGREE

It is the intention of both parties to launch the BACS program in the fall of 2020. We plan to encourage four groups of students to consider pursuing a BACS degree:

(1) Cybersecurity Associate of Applied Science (AAS) Pathway: Students who have completed the MC Cybersecurity AAS program and need to earn a BS degree and gain more specialized cybersecurity knowledge and certifications in order to qualify for certain cybersecurity positions.
(2) 60-Credit Pathway: Students who have completed another (non-Cyber AAS) degree or at least 60 credit hours at MC or another community college or at a four-year school, and who are interested in pursuing cybersecurity careers.
(3) Concurrent Community College (CCC) Pathway: Students who are enrolled at MC or another community college and have completed 30 or fewer credit hours, and who are interested in pursuing cybersecurity careers.
(4) Dual Admission Pathway: Students completing high school who are interested in pursuing a direct pathway to a cybersecurity career.

Each of these pathways is described in more detail below. Program elements shown in blue are to be completed at Montgomery College, while program elements shown red are to be completed at the SANS Technology Institute.

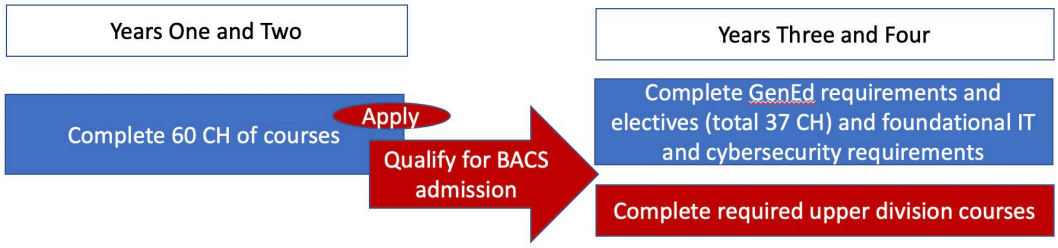
The Cybersecurity AAS Pathway to the BACS



Students who earn the Cybersecurity AAS degree at Montgomery College will have completed most of the foundational (lower division) IT and cybersecurity courses and nearly half the general education courses required to earn the STI Bachelors of Professional Studies in Applied Cybersecurity (BACS) degree. The BACS foundational requirements were designed to correspond seamlessly with the MC Cyber-AAS course requirements, so Cyber-AAS graduates who apply to the BACS program will be accepted provided they have earned a grade point average of at least 3.0 in their Cyber-AAS courses.

BACS students in this pathway will be required to complete 18 additional credit hours of general education courses at MC with a special emphasis on effective writing and speaking, as well as a course on ethics, as shown in the articulation table below (Table 1). Because Cyber-AAS will have completed so many of the BACS-required foundational IT and cybersecurity courses in their first two years at MC, they may enroll in additional advanced upper division cybersecurity electives at STI and/or additional technical or general education electives at MC during their third and fourth years of study.

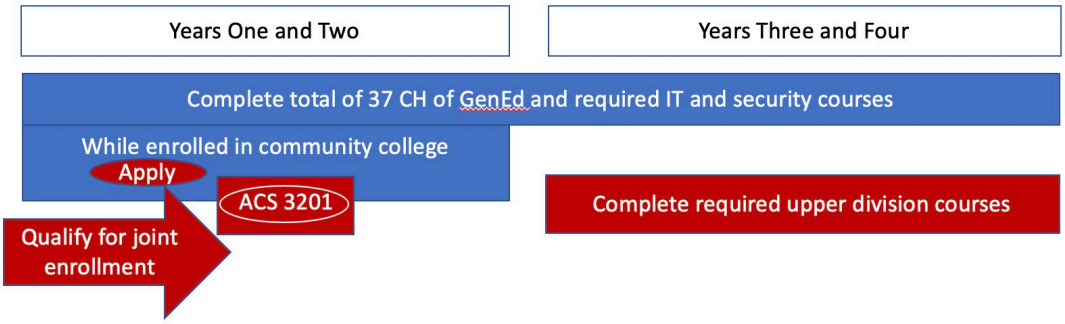
The 60-Credit Pathway to the BACS



The BACS 60 Credit Pathway may be used by any student who has completed an associate's degree (other than the Cyber-AAS) or at least 60 credit hours, with a GPA of at least 3.0, at MC or another community college or at a four-year school. Successful

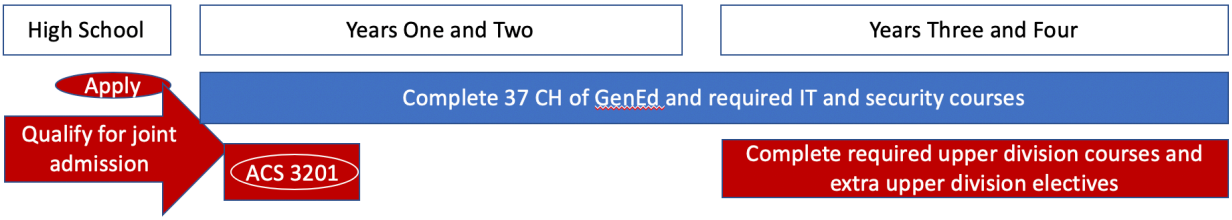
applicants will have demonstrated their aptitude for success in cybersecurity by scoring well on STI's Cyber Talent Examination. Each student accepted into the BACS program will develop a personalized study plan, in consultation with his or her MC and STI advisors for the respective parts of the curriculum, and coordinated by a Program Director. This will allow students to complete all of the required general education and foundational IT and cybersecurity classes they had not yet taken, as well as courses required to meet the BACS general education requirements. Students who have not taken foundational technology courses at a college but have mastered the foundational technologies (such as Linux or networking) may test out of a foundational course by demonstrating hands-on mastery of the specific technology taught in that course through success in earning professional certifications in those technologies. Students who have not completed and cannot test out of some foundational IT and cybersecurity courses may be required to complete more than 60 credit hours of undergraduate courses in order to meet all requirements for the BACS degree.

The Concurrent Community College (CCC) Pathway to the BACS



Students who are enrolled at MC or another community college and who have completed 30 or fewer credit hours, with a GPA of at least 3.0, may apply for early acceptance into STI's BACS program using the STI Cyber Talent Examination to demonstrate their high likelihood of success in cybersecurity. Students who are accepted will develop a personalized study plan, in consultation with their MC and STI advisors, that allows them to complete all of the required general education and foundational IT and cybersecurity classes they had not yet taken, as well as courses required to meet the BACS general education requirements. As soon as is practical after acceptance, CCC students will complete STI's ACS 3201: Technology Essentials course and its associated comprehensive examination, which will help guide their selection of foundational courses. This will allow CCC BACS students to maximize the value from their MC and STI courses.

Dual Admission Pathway to the BACS



Beginning in the 2017–2018 school year, Maryland Governor Larry Hogan and members of his cabinet sponsored an annual Girls Go CyberStart competition in the state to identify young women with aptitude for success in cybersecurity. More than 1,000 Maryland high school girls participated and nearly 20% of them discovered that they not only enjoyed working on the cybersecurity problems but were also good at solving them. Later in 2020, the Girls Go CyberStart program will be paired with a Boys Go CyberStart program, greatly expanding the number of Maryland students who will have the opportunity to demonstrate they are qualified to pursue training and education in cybersecurity. High school seniors who excel in CyberStart, and others who may have developed cybersecurity skills through capture-the-flag and hobbyist activities, may apply for dual admission to MC and STI's BACS program. Dual admission allows students to be immediately accepted into a bachelor's degree program at STI while completing most of their general education and foundational IT and cybersecurity courses at the lower-cost Montgomery College. They can complete their community college courses with confidence that their credits will count toward the 120 credit hours needed for their bachelor's degree, and they will know that their success in the BACS program will mean that they will start their job search with a stronger complement of specialized cybersecurity certifications (at least five specialized GIAC cybersecurity certifications) than nearly any other job candidates.

Students accepted into the dual enrollment program will be assigned both an MC and an STI advisor who, via the liaison activities of the Program Director, will monitor the students' progress through all four years of their college program and help them decide on the most productive path through the MC and STI courses.

Table 1: BACS Program Articulation Roadmap with Montgomery College			
BACS Degree General Education Requirements	**MC Course (credit hours)**	**STI Course (credit hours)**	**General Education or Major**
Arts and Humanities	(3)		General Education
English Composition	(3)		General Education
Social and Behavioral Science	(3)		General Education
Mathematics	(3)		General Education
Biological and Physical Science	(3)		General Education
Interpersonal Communications	COMM 108 (3)		General Education
Business and Professional Communications	COMM 112 (3)		General Education
Research and Writing in the Workplace	ENGL 103 (3)		General Education
Introduction to Ethics	PHIL 140 (3)		General Education
Effective Cyber Writing and Speaking		ACS 4023 (3)	General Education
Four General Education Electives	Transfer (12)		General Education
UNIX/LINUX System Administration	CMSC 253 (3)		Major
Network Operating Systems	NWIT 170 (3)		Major
Windows Server Administration	NWIT 203 (3)		Major
Defending the Network	NWIT 245 (3)		Major
Intermediate Cisco Networking	NWIT 252 (3)		Major
Wireless Security	NWIT 275 (3)		Major
Technology Essentials		ACS 3201 (3)	Major
Introduction to Cybersecurity		ACS 3301 (3)	Major
Security Essentials		ACS 3401 (3)	Major
Automating Information Security with Python		ACS 3573 (3)	Major
Digital Forensics Essentials		ACS 3308 (3)	Major
Incident Handling and Hacker Exploits		ACS 3504 (3)	Major
Three Upper-Division Cybersecurity Specialization Electives		(9)	Major
Eleven IT and Cybersecurity Electives*	(21-33)	(0-12)	Major or General Education
TOTAL BY INSTITUTION	**78 to 90**	**30 to 42**	
TOTAL FOR BACS DEGREE	**120**		

* Where these courses are taken depends on the student's pathway. Students in the Cyber AAS and Dual-Enrollment pathway are expected to take more STI courses.

IV. ADMISSIONS

A. Services

1. STI will provide primary application and admissions services for the Cybersecurity AAS pathway and the 60-credit pathway, including Cyber Talent Examinations for both pathways, supported by MC for the evaluation of general admissibility and transfer credit evaluation.
2. MC will provide primary application and admissions services for the CCC pathway and the Dual Admission pathway, supported by STI for the evaluation of the Cyber Talent Examination and general aptitude for the upper division coursework.
3. MC will evaluate transcripts and provide transfer credit decisions for all applications as they pertain to the MC portion of the curriculum, including transfer credit applicability for all general education credit hours.

B. Program Director

1. STI and MC will both provide a Program Director who will coordinate activities that are necessarily shared between STI and MC, including admissions, advising, and student conduct.

C. Faculty

1. MC faculty will continue to teach all MC courses and STI faculty will continue to teach all upper division courses for students in the BACS program.
2. Through the partnership being fostered by this MOU, MC cybersecurity faculty and STI faculty will establish and nurture an ongoing collegial relationship through the following activities: joint planning of course roadmaps for students in each pathway, MC faculty access to STI's ACS 3201 technology foundations to enable coordinated coverage of topics covered in both programs and to allow MC faculty to recommend improvements to that course, and shared professional development opportunities.

V. STUDENT SERVICES

1. STI will provide the following administrative services and support for students admitted into the BACS program:
    a. Orientation to STI policies, processes, and courses
    b. Basic financial aid and billing support
    c. Career and academic advising
    d. Student conduct proceedings
    e. Graduation services
    f. Alumni services

2. MC will provide the following administrative services and support for BACS-admitted students while they are completing their BACS degree:
    a. Orientation to MC policies, processes, and courses
    b. Registrar services
    c. Basic financial aid and billing support
    d. Transfer course processing
    e. Student conduct proceedings
3. STI and MC program directors will meet at least quarterly to review the progress of each BACS student in order to conduct program coordination as needed.

VI. COMMUNICATIONS, MARKETING, AND RECRUITMENT

1. STI and MC will both actively recruit students to the BACS program, with a focus on the breakdown of admissions pathways as described above in Section IV.
    a. STI recruitment efforts will include visits to Montgomery College, online information sessions, email marketing, and social media marketing.
    b. MC will include STI BACS program marketing materials during activities such as visits to high schools by its recruiters, college fairs, and open houses and campus tours.
    c. STI will support and coordinate with MC recruitment efforts as requested.
2. Both parties agree that marketing materials and other communications must accurately represent the program and the roles of each of the partners. This includes press releases, brochures, public presentations, etc. STI will have the overall coordination responsibility for these materials. MC and STI will each designate representatives from its institution to collaborate with the designated BACS marketing lead at STI.
3. STI and MC will work together to expand knowledge about the BACS program among faculty and administration at other community colleges in Maryland and encourage them to work with STI and MC to enable their students to take advantage of the program by using MC courses to enable their students to complete any BACS-required foundational or general education courses not currently offered at their colleges.
4. In order to encourage broader access to the BACS program, MC will consider offering Maryland students from outside Montgomery County in-county tuition pricing for MC courses required for the BACS.

VII. OTHER MANAGEMENT TOPICS

1. STI and MC intend to conduct research on the educational outcomes of the BACS program and publish papers and present at conferences about it. The two

institutions expect to pursue grant funding opportunities as they may arise to enhance the BACS program,

2. STI and MC agree to ongoing collaboration to ensure that the integrity of the BACS program as articulated between the two institutions shall continue to meet industry standards and specifications.
3. All parties to this agreement agree to work together to resolve any program issues through joint input, collaboration, and negotiation.

VIII. ADMINISTRATION OF PROGRAM

STI Administrator:

1. Betsy Marchant, Assistant Director, SANS Technology Institute

MC Administrator:

1. Margaret Latimer, Vice President and Provost, Collegewide STEM Unit and Germantown Campus, Montgomery College

IX. FORCE MAJEURE

If either party's performance(s) hereunder is rendered impossible, hazardous, or is otherwise prevented or impaired due to sickness, inability to perform, accident, interruption or failure of means of transportation, Act(s) of God, riots, strikes, labor difficulties, war (including civil war), embargoes, epidemics, fires, floods, explosions, earthquakes, quarantine restrictions, any act or order of any civil or military authority, acts of any government, and/or any other cause or event, similar or dissimilar, beyond that party's control, then each party's obligations with respect to the affected performance(s) shall be excused and neither party will have any liability in connection therewith.

X. GOVERNING LAW AND FORUM

The terms of this Agreement shall be governed by the Laws of the State of Maryland of the United States. Any dispute arising from this Agreement that is not resolved by agreement of the parties shall be resolved exclusively in the Courts and regulatory agencies of the State of Maryland of the United States.

XI. TERM RENEWAL AND TERMINATION OF AGREEMENT

This agreement becomes effective upon signature by authorized representatives of MC, and STI. It remains in effect until June 30, 2024. The parties will discuss and negotiate during Academic Year 2022–2023 the renewal, extension, or modification of the MOU in

order to achieve the best path forward for the BACS program.

This MOU may be modified only by mutual written agreement of all parties.

XII. CORRESPONDENCE

In the interest of implementing this MOU in a systematic manner, STI and MC will each designate a contact person assigned the responsibility of coordinating MOU activities in general terms.

STI: Eric Patterson, Executive Director, SANS Technology Institute

MC: Margaret Latimer, Vice President and Provost, Collegewide STEM Unit and Germantown Campus, Montgomery College

XIII. DATE OF AGREEMENT/SIGNATURES ON AGREEMENT/AUTHORITY TO EXECUTE

This Agreement is dated as of _____ and will become effective upon signature by the authorized representatives of the parties. The undersigned individuals represent and warrant that they are expressly and duly authorized by their respective institutions to execute the Agreement.

XIV. REQUIRED SIGNATURE

The parties identified below agree to the provisions and terms of this MOU.

APPROVED:

_____	_____
Eric Patterson Date	Margaret Latimer Date
Executive Director	Vice President and Provost
SANS Technology Institute	Collegewide STEM Unit
	Germantown Campus, Montgomery College