SANS Technology Institute

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

ED SKOUDIS
President

DAVID HOELZER
Dean of Faculty

JOHANNES ULLRICH, Ph.D.
Dean of Research

ERIC PATTERSON
Provost

BETSY MARCHANT
Vice Provost

September 20, 2023

Sanjay K. Rai, 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. Rai,

The SANS Technology Institute is pleased to submit the attached proposal to create a new Software Supply Chain Security post-baccalaureate certificate program. As the only program of its kind in Maryland, this post-baccalaureate certificate will provide students the knowledge and training to support and lead organizations in securely designing, writing, packaging, and deploying software.

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

Ed Skoudis
President
SANS Technology Institute

PROPOSAL FOR A
POST-BACCALAUREATE CERTIFICATE IN
SOFTWARE SUPPLY CHAIN SECURITY

SANS Technology Institute

MHEC
ENGAGE • INFORM • SUPPORT

Office Use Only: PP#

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

Institution Submitting Proposal	SANS Technology Institute

Each action below requires a separate proposal and cover sheet.

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

Payment Submitted:	● Yes ○ No	Payment Type:	○ R*STARS # 190484 ● Check # 190484	Payment Amount:	$850	Date Submitted:	9/29/23

Department Proposing Program	SANS Technology Institute	
Degree Level and Degree Type	Post-baccalaureate Certificate	
Title of Proposed Program	Software Supply Chain Security	
Total Number of Credits	12	
Suggested Codes	HEGIS: 5199.00	CIP: 11.1003
Program Modality	○ On-campus ○ Distance Education (fully online) ● Both	
Program Resources	● Using Existing Resources ○ Requiring New Resources	
Projected Implementation Date (must be 60 days from proposal submission as per COMAR 13B.02.03.03)	○ Fall ● Spring ○ Summer Year: 2024	
Provide Link to Most Recent Academic Catalog	URL: https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltd95c29b887b4bd7e/Graduate-Course-Catalog.pdf	

Preferred Contact for this Proposal	Name:	Thomas Vanderhorst
	Title:	Director of Academic Affairs
	Phone:	(301) 371-2142
	Email:	tvanderhorst@sans.edu

President/Chief Executive	Type Name: Ed Skoudis
	Signature: Date: 09/20/2023
	Date of Approval/Endorsement by Governing Board: 08/14/2023

Revised 1/2021

Table of Contents

A. Centrality to Institutional Mission Statement and Planning Priorities

1. Program Description

The SANS Technology Institute (STI) proposes to launch a new program leading to a Post-Baccalaureate Certificate in Software Supply Chain Security. The proposed SANS Technology Institute post-baccalaureate certificate program is a 12-credit hour program with a cohesive set of learning outcomes focused on teaching secure development applied concepts, skills, and technologies.

Software Supply Chain Security post-baccalaureate certificate students will complete three required core courses and one elective courses, earning four 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 eight other post-baccalaureate certificate programs. Software Supply Chain Security post-baccalaureate 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 post-baccalaureate certificate programs can be found online at https://www.sans.edu/admissions/certificates.

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

The proposed post-baccalaureate certificate program aligns well with STI's mission and vision.

Our mission calls for us to graduate "technically-skilled professionals and leaders who strengthen global information security" who can, according to our vision, "perform leading-edge research that identifies current best practices and enhances the state of the art in the practice of information security" 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."

3. Funding for the Program

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

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

The Software Supply Chain Security program will be critically valuable to STI in meeting its top strategic objective of increasing the number of technically-skilled professionals and leaders. Thus, the program has and will continue to have the highest visibility and priority for STI's president, management, and administrative staff.

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

1. Critical Need for the Software Supply Chain Security Program

Developers struggle to design security into their software as they face competing priorities. Two–thirds of the participants of a recent industry survey admitted they routinely left known vulnerabilities and exploits in their code, and only 14% listed application security as a top priority.

Many reasons exist for this lack of prioritization of software supply chain security, including increasing code complexity, company culture, and development methodology, but if it remains an underlying truth that most code developers simply lack security skills, then all other factors are moot.

In that same recent survey, 92% of respondents indicated that their team required more training in security frameworks, and more than half reported a lack of familiarity with common software vulnerabilities, how they can be exploited, and methods for avoiding them.

Across all of Maryland's institutions of higher education, only Capitol Technology University indicates within the MHEC program inventory that they offer a post-baccalaureate certificate in Secure Software Development, however that institution's website would seem to indicate that they do not in fact still actually offer that program (https://www.captechu.edu/degrees-and-programs/certificates). Thus, Maryland is effectively outsourcing its reliance for secure coding talent to other states. This program would begin to address that shortfall.

2. Alignment with the 2022 Maryland State Plan for Higher Education

This program directly supports Priority 5 of the 2022 Maryland State Plan for Higher Education: *Maintain the commitment to high-quality postsecondary education in Maryland*.

Building upon our existing world-class SANS courses and GIAC exams and creating a coherent and logical sequence of courses to address a skills gap in Maryland's workforce which contributes to an existential threat, this program offers the same narrowly focused, hands-on, practical, and high-quality education which our students experience and benefit from in our existing programs.

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

1. **Market Demand, and**
2. **Demand for Software Supply Chain Security Graduates**

Within the field of Information Technology, there is an estimated 26.9 million professional software engineers across the world as of 2022, up from 21 million in 2016. In the United States alone, there are approximately 4.4 million professional software engineers as of 2022.[1]

Generally, developer groups make up a large portion of an organization's technical team. It's not uncommon for a single, large Enterprise organization to have anywhere from 25-250 developers, *or more.*

Despite recent layoffs, organizations are still actively seeking to fulfill developer positions. What's more, many organizations are citing a "Developer Shortage", which indicates a critical need for developers, from an industry-wide perspective.[2, 3, 4]

Lack of Secure Developers
Not only are developers in high demand, *but developers that understand security are in even higher demand.*[5, 6, 7, 8]

Within the past few years, the industry has shifted its focus on application and web application security due to an increased number of attacks, exploits, and vulnerabilities related to software, applications, and elements within the ***Software Development Lifecycle*** and respective ***software supply chains***.

Apache Struts 2[9] and log4j[10] are larger, more well-known occurrences.

The 2022 Verizon Data Breach Investigations Report[11] identified that basic web application attacks as the second most common way attackers have compromised systems.

[1] Software Engineering Demographics, Wikipedia. https://en.wikipedia.org/wiki/Software_engineering_demographics#:~:text=Software%20engineers%20form%20part%20of,from%2021%20million%20in%202016
[2] Software Developer Statistics 2023, True List: https://truelist.co/blog/software-development-statistics/
[3] Future of Software Engineering 2023 and Beyond, Knowledge Hut: https://www.knowledgehut.com/blog/web-development/software-engineer-future#:~:text=In%202023%2C%20the%20demand%20for,it%20more%20effective%20and%20accurate
[4] Why Software Developer is the Number 1 Job in 2023: https://money.usnews.com/careers/articles/why-software-developer-is-the-no-1-job-of-2023
[5] The Rising Demand for DevSecOps Talent, DevOps[dot]com: https://devops.com/the-rising-demand-for-devsecops-talent/
[6] DevSecOps to Explode in 2023, Guard Rails: https://www.guardrails.io/blog/the-devsecops-market-is-set-to-explode-in-2023-heres-why/
[7] The Rising Demand for DevSecOps, Forbes: https://www.forbes.com/sites/forbestechcouncil/2023/02/22/the-rising-demand-for-devsecops-talent-recruiting-and-retaining-skilled-developers/?sh=6cb020862e4c
[8] Software Engineering Statistics, Kinsta: https://kinsta.com/software-engineering-statistics/
[9] SANS on Struts2 Attacks: https://www.sans.org/webcasts/struts-shock-current-attacks-struts2-defend-104787/
[10] SANS on log4j Vulnerability: https://www.sans.org/blog/what-do-you-need-to-know-about-the-log4j-log4shell-vulnerability/
[11] 2022 Verizon Data Breach Investigations Report: https://www.verizon.com/business/resources/reports/dbir/interactive/

Furthermore, on April 28th, 2023, CISA launched a ***Secure Software Development Attestation Form***[12] as a template to outline secure software development practices and mandate a set of standards for Federal agencies to abide by. Sufficient to say, it's a commonality for certain standards to start within the realm of government and military and later become an expectation of the corporate world, too. More guidance like this is likely to become more and more frequent as newer vulnerabilities, exploits, and subsequent breaches continue to surface.

3. 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 this challenging field. This growth will call for educated technical leaders with diverse skillsets and the ability to implement, develop, integrate, orchestrate, and lead cloud security operations.

While many institutions offer cybersecurity courses and programs, these offerings are admittedly often reactive in nature; that is, cybersecurity practitioners most typically respond to threats and incidents rather than mitigate the root cause contributor of weak and vulnerable coding. The previous analysis of market demographics and demand (Section C1) demonstrates that there is a ready supply of potential graduates from this proposed program.

D. Reasonableness of Program Duplication

1. Similarities and Differences between the Software Supply Chain Security 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.

[12] Secure Software Development Attestation Form: https://www.cisa.gov/sites/default/files/2023-04/secure-software-self-attestation_common-form_508.pdf

Currently, we are unaware of any educational program which is specifically seeking to produce practitioners who are specifically prepared for software supply chain security. The STI Software Supply Chain Security post-baccalaureate certificate program is intended to provide that opportunity, especially for those already employed in the field who require focused and specialized training in this area to build upon and supplement their general development and cybersecurity education and experience.

Our analysis of these factors clearly demonstrates that the STI Software Supply Chain Security 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
COMPUTER PROGRAMMING/PROGRAMMER, GENERAL - 110201
COMPUTER PROGRAMMING, SPECIFIC APPLICATIONS - 110202
COMPUTER PROGRAMMING, OTHER - 110299
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. Across all of Maryland's institutions of higher education, only Capitol Technology University indicates within the MHEC program inventory that they offer a post-baccalaureate certificate in Secure Software Development, however that institution's website would seem to indicate that they do not in fact still actually offer that program (https://www.captechu.edu/degrees-and-programs/certificates).

Degree to Be Awarded

Post-baccalaureate 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 Software Supply Chain Security program will hold four industry-recognized GIAC certifications in addition to their post-baccalaureate 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 Software Supply Chain Security 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.

2. Admissions Requirements

STI's admission requirements for Software Supply Chain Security program will be as already established for our existing post-baccalaureate certificate programs:

- Have at least 12 months of professional work experience in information technology or information security.
- 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 Software Supply Chain Security 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. Describe how the proposed program was established, and also describe the faculty who will oversee the program.

The Software Supply Chain Security program was established as a means of meeting STI's strategic goal of "materially increasing the number of technically skilled professionals and leaders who strengthen global information security through innovative and flexible approaches to learning." Our faculty and administrators recognized the need for a program that guides students to become secure developers who can apply sound cybersecurity principles and processes in all phases of the Software Development Lifecycle. As shown in the Critical Need (B.1.) and Market Demand (C.1.) sections, there is a vital shortage of secure developers and a concerning lack of educational programs to support them. Our Faculty Committee and administrators brought together the key faculty members with the relevant expertise and experience in secure development to create the right combination of courses necessary for this unique program.

STI’s current faculty leadership who support this proposed Software Supply Chain Security post-baccalaureate certificate program includes the following individuals:

Eric Johnson (ISE 6650 and ISE 6612)

Eric Johnson is a co-founder and principal security engineer at Puma Security focusing on modern static analysis product development and DevSecOps automation. His experience includes application security automation, cloud security reviews, static source code analysis, web and mobile application penetration testing, secure development lifecycle consulting, and secure code review assessments.

Previously, Eric spent 5 years as a principal security consultant at an information security consulting firm helping companies deliver secure products to their customers, and another 10 years as an information security engineer at a large US financial institution performing source code audits.

As a Senior Instructor with the SANS Institute, Eric authors information security courses on DevSecOps, cloud security, secure coding, and defending mobile apps. He serves on the advisory board for the SANS Security Awareness Developer training program, delivers security training around the world, and presents security research at conferences including SANS, BlackHat, OWASP, BSides, JavaOne, UberConf, and ISSA.

Eric completed a BS degree in Computer Engineering and a MS in Information Assurance at Iowa State University, and currently holds the CISSP, GWAPT, GSSP-.NET, and GSSP-Java certifications.

Frank Kim (ISE 6650)

Frank Kim is the Founder of ThinkSec, a security consulting and CISO advisory firm, as well as a SANS Faculty Fellow and lead for both the SANS Management and SANS Cloud Security curricula, overseeing two dozen SANS courses in the two fastest growing curricula.

Previously, as CISO at the SANS Institute, Frank led the information risk function for the most trusted source of computer security training and certification in the world.

Frank is also the author and instructor of MGT512: Security Leadership Essentials for Managers, MGT514: Security Strategic Planning, Policy, and Leadership, and co-author of SEC540: Cloud Security and DevOps Automation.

Frank began his career as a developer in the early days of the Internet building applications and systems. When incidents would occur and vulnerabilities were discovered, Frank became the default point person for managing them. Though he did not realize it at the time, this was the beginning of his professional career in security. As his career progressed, he built teams both large and small to solve some interesting problems. This included forming a multi-million-dollar security program at Kaiser Permanente as the Executive Director of Cybersecurity where he built an innovative security program to meet the unique needs of the nation's largest not-for-profit health plan and integrated health care provider with annual revenue of $60 billion, 10 million members, and 175,000 employees.

Frank holds a BA in Ethnic studies and a MBA from the University of California at Berkeley, is a frequent speaker at the annual RSA Conference, and has earned a number of professional certifications including: CISSP, GSLC, GCIH, GCIA, GCFA, GPEN, and GSSP.

Johannes Ullrich (ISE 6615)

Johannes Ullrich, one of only fourteen SANS Faculty Fellows, is currently responsible for the SANS Internet Storm Center (ISC) and the GIAC Gold program. In 2000, he founded DShield.org, which is now the data collection engine behind the ISC. His work with the ISC has been widely recognized, and in 2004, *Network World* named him one of the 50 most powerful people in the networking industry. Prior to working for SANS, Johannes worked as a lead support engineer for a web development company and as a research physicist. Johannes holds a PhD in physics from SUNY Albany and is based in Jacksonville, Florida. His daily Internet Storm Center podcast, which is downloaded tens of thousands of times per day, summarizes current security news in a concise format.

Mark Baggett (ISE 6350)

Mark Baggett is a SANS Senior Instructor and is the course author and primary instructor for SEC573: Automating Information Security with Python and for SEC673: Advanced Information Security Automation with Python.
Mark has a master's degree in information security engineering from the SANS Technology Institute and is the 15th person in the world to receive the prestigious GIAC Security Expert certification (GSE). He also holds GPYC, GXPN, GPEN, GCIA, GCIH, GSEC, GWAPT, and GCPM certifications.

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

Ryan Nicholson (ISE 6610)

Ryan started his information technology career as a system administrator for the US Department of Defense and quickly took on a more security-focused role as the field office's Network Security Officer, eventually becoming a cybersecurity lead auditor.

As the lead cybersecurity engineer for a major DoD cloud project, he constantly learned new and exciting methods to ensure that information systems in both an off- and on-premises environment can be adequately defended. He continues providing support to this government contractor but is now employed by SANS as a senior technical advisor for the Blue Team Operations curriculum team.

Ryan has earned several industry certifications, including GIAC's GDSA, GWAPT, GCIH, GSLC, and GSEC, Offensive Security's OSCP, ISC2's CISSP, EC Council's CEH and CFHI, and AWS' Certified Solutions Architect Associate.

Ryan earned his BS in Computer Science, with a concentration in Software Engineering, from Shippensburg University of Pennsylvania and his MS in Cybersecurity and Information Assurance from Western Governor's University.

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

The five primary educational objectives of the program are to:

a) PLO1: Understand the importance of a "***Security First***" or "***Shift Left***" mindset.
b) PLO2: Have a greater understanding of public cloud platforms and infrastructure.
c) PLO3: Recognize and mitigate common application and web application attacks.
d) PLO4: Holistically secure ***Software Development Lifecycles*** (SDLC), APIs, and microservices.
e) PLO5: Better implement and automate security, infrastructure, compliance, and auditing capabilities.

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

PLO 1: ISE 6650 Cloud Security and DevOps Automation

- ISE 6650 teaches students how implementing the principles, practices, and tools of DevOps can improve the reliability, integrity, and security of on-premises and cloud-hosted applications.

PLO 2: ISE 6612 Public Cloud Security

- ISE 6612 provides students with an in-depth understanding of the inner workings of the most popular public cloud providers: AWS, Microsoft Azure, and GCP.

PLO 3: ISE 6615 Defending Web Applications Security Essentials

- ISE 6615 teaches students common security flaws in modern web applications and how to recognize and mitigate these flaws early and efficiently.

PLO 4: ISE 6615 Defending Web Applications Security Essentials

- ISE 6615 teaches students to efficiently mitigate risks of web application and exposure and compromise of sensitive data by adding security early in the software development life cycle, "shifting left" security decisions, and testing.

PLO 5: ISE 6650 Cloud Security and DevOps Automation

- ISE 6650 provides students with a deep understanding of and hands-on experience with the DevOps methodology used to build and deliver cloud infrastructure and software. Students learn how to attack and then harden the entire DevOps workflow, from version control to continuous integration and running cloud workloads. It also teaches and provides hands-on experience in using popular open-source tools to automate Configuration Management ("infrastructure as Code"), Continuous Integration (CI), Continuous Delivery (CD), containerization, micro-segmentation, automated compliance ("Compliance as Code"), and Continuous Monitoring.

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

Each program learning outcome and course objective listed above is measured by the respective GIAC certification examination associated with each of the three core courses that the student completes from those listed in Section G.4.

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.

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

Required Courses

Required core courses (9 credit hours):

Students will take these three core courses:
ISE 6650 (SANS Course SEC540): Cloud Security and DevSecOps Automation | GCSA: GIAC Cloud Security Automation (3 credits)
ISE 6612 (SANS Course SEC510): Public Cloud Security: AWS, Azure, and GCP | GPCS: GIAC Public Cloud Security (3 credits)
ISE 6615 (SANS Course SEC522): Defending Web Applications Security Essentials | GWEB: GIAC Web Application Defender (3 credits)

ISE 6650 Cloud Security and DevOps Automation (3 credits)

SANS class: SEC540, Cloud Security and DevOps Automation
Assessment: GIAC Cloud Security Automation (GCSA)
3 Credit Hours

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

This course will prepare students to:

- Understand how DevOps works and identify keys to success
- Wire security scanning into automated CI/CD pipelines and workflows
- Build continuous monitoring feedback loops from production to engineering
- Automate configuration management using Infrastructure as Code (IaC)
- Secure container technologies (such as Docker and Kubernetes)
- Use native cloud security services and third-party tools to secure systems and applications
- Securely manage secrets for Continuous Integration servers and applications
- Integrate cloud logging and metrics
- Perform continuous compliance and security policy scanning

ISE 6612 Public Cloud Security: AWS, Azure, and GCP (3 credits)

SANS class: SEC510, Public Cloud Security: AWS, Azure, and GCP
Assessment: GIAC Public Cloud Security (GPCS)
3 Credit Hours

ISE 6612 teaches students how the major cloud providers work and how to securely configure and use their services and Platform as a Service (PaaS) offerings.

Organizations in every sector are increasingly adopting cloud offerings to build their online presence. However, although cloud providers are responsible for the security of the cloud, their customers are responsible for what they do in the cloud. Unfortunately, the providers have made the customer's job difficult by offering many services that are insecure by default. Worse yet, with each provider offering hundreds of different services and with many organizations opting to use multiple providers, security teams need a deep understanding of the underlying details of the different services to lock them down. As the landscape rapidly evolves and development teams eagerly adopt the next big thing, security is constantly playing catch-up to avert disaster.

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

The Big 3 cloud providers alone provide more services than any one company can consume. As security professionals, it can be tempting to limit what the developers use to the tried-and-true solutions of yesteryear. Unfortunately, this approach will inevitably fail as the product development organization sidelines a security entity that is unwilling to change. Functionality drives adoption, not security, and if a team discovers a service offering that can help get its product to market quicker than the competition, it can and should use it. This course gives students the ability to provide relevant and modern guidance and guardrails to these teams to enable them to move both quickly and safely.

This course will prepare students to:

- Understand the inner workings of cloud services and Platform as a Service (PaaS) offerings in order to make more informed decisions in the cloud
- Understand the design philosophies that undergird each provider and how these have influenced their services in order to properly prescribe security solutions for them
- Discover the unfortunate truth that many cloud services are adopted before their security controls are fully fleshed out
- Understand Amazon Web Services (AWS), Azure, and Google Cloud Platform (GCP) in depth.
- Understand the intricacies of Identity and Access Management, one of the most fundamental concepts in the cloud and yet one of the last understood
- Understand cloud networking and how locking it down is a critical aspect of defense-in-depth in the cloud
- Analyze how each provider handles encryption at rest and in transit in order to prevent sensitive data loss
- Explore the service offering landscape to discover what is driving the adoption of multiple cloud platforms and to assess the security of services at the bleeding edge
- Understand the complex connections between cloud accounts, providers, and on-premise systems and the cloud
- Perform secure data migration to and from the cloud

ISE 6615 Defending Web Applications Security Essentials (3 credits)

SANS class: SEC 522, Application Security: Securing Web Apps, APIs, and Microservices
Assessment: GIAC Web Application Defender (GWEB)
3 Credit Hours

Web applications are increasingly distributed. What used to be a complex monolithic application hosted on premise has become a distributed set of services incorporating on-premises legacy applications along with interfaces to cloud-hosted and cloud-native components. Because of this coupled with a lack of security knowledge, web applications are exposing sensitive corporate data. Security professionals are asked to provide validated and scalable solutions to secure this content in line with best industry practices using modern web application frameworks. Attending this class will not only raise awareness about common security flaws in modern web applications, but it will also teach students how to recognize and mitigate these flaws early and efficiently.

During the course, instructors demonstrate the risks of web applications and the extent of sensitive data that can be exposed or compromised. From there, they offer real world solutions on how to mitigate these risks and effectively evaluate and communicate residual risks. After attending the class, students will be able to apply what they learned quickly and bring back techniques to not only better secure their applications, but also do so efficiently by adding security early in the software development life cycle, "shifting left" security decisions and testing, thus saving time, money, and resources for the organization.

This course will prepare students to:

- Defend against the attacks specified in OWASP Top 10
- Infrastructure security and configuration management

- Securely integrating cloud components into a web application
- Learn about Authentication and authorization mechanisms, including single sign-on patterns
- Understand cross-domain web request security
- Leverage protective HTTP headers
- Defending SOAP, REST and GraphQL APIs
- Securely implement Microservice architecture
- Defending against input related flaws such as SQL injection, XSS and CSRF

Electives Courses: (3 credit hours)

Students will select one of the following elective course options:

ISE 6610 (SANS Course SEC 488): Cloud Security Essentials | GCLD: GIAC Cloud Security Essentials (3 credits) **If chosen as an elective, this course must be taken first*
ISE 6630 (SANS Course SEC 588): Cloud Penetration Testing | GCPN: GIAC Cloud Penetration Tester (3 credits)
ISE 6315 (SANS Course SEC542): Web App Penetration Testing and Ethical Hacking | GWAPT: Web Application Penetration Tester (3 credits)
ISE 6350 (SANS Course SEC573): Automating Information Security with Python | GPYC: Python Coder (3 credits)
ISE 6715 (SANS Course AUD507): Auditing & Monitoring Networks, Perimeters, & Systems | GSNA: Systems and Network Auditor (3 credits)
ISE 5800 (SANS Course MGT525): IT Security Project Management | GCPM: Certified Project Manager (3 credits)

ISE 6610 Cloud Security Essentials (3 credits)

SANS class: SEC 488, Cloud Security Essentials
Assessment: GIAC Cloud Security Essentials (GCLD)
3 Credit Hours

ISE 6610, Cloud Security Essentials. New technologies introduce new risks. This course will equip students to implement appropriate security controls in the cloud, often using automation to "inspect what you expect." Mature CSPs have created a variety of security services that can help customers use their products in a more secure manner, but much about cloud security still resides with the customer organization. This course covers real-world lessons using security services created by the CSPs as well as open-source tools. Each lesson features hands-on lab exercises to help students practice the lessons learned. Students will progressively layer multiple security controls in order to end the course with a functional security architecture implemented in the cloud.

The course begins by addressing one of the most crucial aspects of the cloud - Identity and Access Management (IAM). From there, students will learn to secure the cloud through discussion and practical, hands-on exercises related to several key topics to defend various cloud workloads operating in the different CSP models of: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

This course will prepare students to:

- Identify the risks and risk control ownership based on the deployment models and service delivery models of the various products offered by cloud service providers (CSPs).
- Evaluate the trustworthiness of CSPs based on their security documentation, service features, third-party attestations, and position in the global cloud ecosystem.
- Create accounts and use the services of any one the leading CSPs and be comfortable with the self-service nature of the public cloud, including finding documentation, tutorials, pricing, and security features.
- Articulate the business and security implications of a multi-cloud strategy.
- Secure access to the consoles used to access the CSP environments.
- Use command line interfaces to query assets and identities in the cloud environment.
- Use hardening benchmarks, patching, and configuration management to achieve and maintain an engineered state of security for the cloud environment.
- Evaluate the logging services of various CSPs and use those logs to provide the necessary accountability for events that occur in the cloud environment.
- Configure the command line interface (CLI) and properly protect the access keys to minimize the risk of compromised credentials.
- Use basic Bash and Python scripts to automate tasks in the cloud.
- Implement network security controls that are native to both AWS and Azure.
- Employ an architectural pattern to automatically create and provision patched and hardened virtual machine images to multiple AWS accounts.
- Use Azure Security Center to audit the configuration in an Azure deployment and identify security issues.
- Use Terraform to deploy a complete "infrastructure as code" environment to multiple cloud providers.
- Leverage the Cloud Security Alliance Cloud Controls Matrix to select the appropriate security controls for a given cloud network security architecture and assess a CSP's implementation of those controls using audit reports and the CSP's shared responsibility model.
- Follow the penetration testing guidelines put forth by AWS and Azure to invoke your "inner red teamer" to compromise a full stack cloud application
- Use logs from cloud services and virtual machines hosted in the cloud to detect a security incident and take appropriate steps as a first responder according to a recommended incident response methodology.
- Perform a preliminary forensic file system analysis of a compromised virtual machine to identify indicators of compromise and create a file system timeline.

ISE 6630 Cloud Penetration Testing (3 credits)

SANS class: SEC 588 Cloud Penetration Testing
Assessment: GIAC Cloud Penetration Tester (GCPN)
3 Credit Hours

Computing workloads have been moving to the cloud for years. Analysts predict that most, if not all, companies will have soon have workloads in public and other cloud environments. While organizations that start in a cloud-first environment may eventually move to a hybrid cloud and local data center solution, cloud usage will not decrease significantly. So when assessing risks to an organization going forward, we need to be prepared to evaluate the security of cloud-delivered services.

The most asked questions regarding cloud security when it comes to penetration testing are: Do I need to train specifically for engagements that are cloud-specific? and Can I accomplish my objectives with other pen test training and apply it to the cloud? In cloud-service-provider environments, penetration testers will not encounter a traditional data center design, there will be new attack surface areas in the service (control) planes of these environments. Learning how such an environment is designed and how you as a tester can assess what is in it is a niche skill set that must be honed. What we rely on to be true in a classical data center environment such as who owns the Operating System and the infrastructure and how the applications are running will likely be very different. Applications, services, and data will be hosted on a shared hosting environment unique to each cloud provider.

The course dives into topics of classic cloud Virtual Machines, buckets, and other new issues that appear in cloud-like microservices, in-memory data stores, files in the cloud, serverless functions, Kubernetes meshes, and containers. It also covers Azure and AWS penetration testing, which is particularly important given that AWS and Microsoft account for more than half of the market. The goal is not to demonstrate these technologies but to teach students how to assess and report on the actual risk their organizations could face if these services are left insecure.

This course will prepare students to:

- Conduct cloud-based penetration tests
- Assess cloud environments and bring value back to the business by locating vulnerabilities
- Understand first-hand how cloud environments are constructed and how to scale factors into the gathering of evidence
- Assess security risks in Amazon and Microsoft Azure environments, the two largest cloud platforms in the market today

ISE 6315 Web App Penetration Testing and Ethical Hacking (3 credits)

SANS class: SEC 542, Web App Penetration Testing and Ethical Hacking
Assessment: GIAC Web Application Penetration Tester (GWAPT)
3 Credit Hours

Web applications play a vital role in every modern organization. But, if an organization does not properly test and secure its web apps, adversaries can compromise these applications, damage business functionality, and steal data. Unfortunately, many organizations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems.

Students will come to understand common web application flaws, as well as how to identify and exploit them with the intent of demonstrating the potential business impact. Along the way, students follow a field-tested and repeatable process to consistently find flaws. Information security professionals often struggle with helping their organizations understand risk in terms relatable to business. The goal of SEC542 is to better secure organizations through penetration testing, and not just show off hacking skills. The course will help students demonstrate the true impact of web application flaws not only through exploitation but also through proper documenting and reporting.

In addition to walking students through a web app penetration using more than 30 formal hands-on labs, the course culminates in a web application pen test tournament, powered by the SANS Netwars cyber range. This Capture-the-Flag event groups students into teams to apply their newly acquired command of web application penetration testing techniques in a fun way that hammers home lessons learned throughout the course.

This course will prepare students to:

- Apply OWASP's methodology to your web application penetration tests to ensure they are consistent, reproducible, rigorous, and under quality control.
- Analyze the results from automated web testing tools to validate findings, determine their business impact, and eliminate false positives.
- Manually discover key web application flaws.
- Use Python to create testing and exploitation scripts during a penetration test.
- Discover and exploit SQL Injection flaws to determine true risk to the victim organization.
- Understand and exploit insecure deserialization vulnerabilities with ysoserial and similar tools.
- Create configurations and test payloads within other web attacks.
- Fuzz potential inputs for injection attacks with ZAP, BurP'S Intruder and ffuf.
- Explain the impact of exploitation of web application flaws.
- Analyze traffic between the client and the server application using tools such as the Zed Attack Proxy and BurpSuite Pro to find security issues within the client-side application code.
- Manually discover and exploit Cross-Site Request Forgery (CSRF) attacks.
- Manually discover and exploit Server-Side Request Forgery (SSRF) attacks.
- Use the Browser Exploitation Framework (BeEF) to hook victim browsers, attack client software and the network, and evaluate the potential impact that XSS flaws have within an application.
- Use the Nuclei tool to perform scans of target web sites/servers.
- Perform two complete web penetration tests, one during the five sections of course instruction, and the other during the Capture the Flag exercise.

ISE 6350 Automating Information Security with Python (3 credits)

SANS class: SEC573, Automating Information Security with Python
Assessment: GIAC Python Coder (GPYC)
3 Credit Hours

Python is a simple, user-friendly language that is designed to make it quick and easy to automate the tasks performed by security professionals. Whether you are new to coding or have been coding for years, SEC573 will have you creating programs that make your job easier and your work more efficient. This self-paced course starts from the very beginning, assuming you have no prior experience or knowledge of programming. We cover all of the essentials of the language up front. If you already know the essentials, you will find that the pyWars lab environment allows advanced developers to quickly accelerate to more advanced course material.

SEC573 is designed to give students the skills they need to tweak, customize, or outright develop their own tools. We put students on the path to create their own tools, empowering them to better automate the daily routine of today's information security professional and achieve more value in less time. Again and again, organizations serious about security emphasize their need for skilled tool builders. There is a huge demand for people who can understand a problem and then rapidly develop prototype code to attack or defend against it.

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

This course will prepare students to:

- Leverage Python to perform routine tasks quickly and efficiently
- Automate log analysis and packet analysis with file operations, regular expressions, and analysis modules to find evil
- Develop forensics tools to carve binary data and extract new artifacts
- Read data from databases and the Windows Registry
- Interact with websites to collect intelligence
- Develop UDP and TCP client and server applications
- Automate system processes and process their output

ISE 6715 Auditing & Monitoring Networks, Perimeters, & Systems (3 credits)

SANS class: AUD507, Auditing & Monitoring Networks, Perimeters, & Systems
Assessment: GIAC Systems and Network Auditor (GSNA)
3 Credit Hours

This course is organized specifically to provide a risk-driven method for tackling the enormous task of designing an enterprise security validation program, covering systems, applications, and the cloud. After covering a variety of high-level audit issues and general audit best practices, students will have the opportunity to delve into the technical "how-to" for determining the key controls that can be used to provide a high level of assurance to an organization. Real-world examples provide students with tips on how to verify these controls in a repeatable way, as well as many techniques for continuous monitoring and automatic compliance validation. These same real-world examples help the students learn how to be most effective in communicating risk to management and operations staff.

Students will leave the course with the know-how to perform effective tests of enterprise security in a variety of areas including systems, applications, and the cloud. The combination of high-quality course content, provided audit checklists, in-depth discussion of common audit challenges and solutions, and ample opportunities to hone their skills in the lab provides a unique setting for students to learn how to be an effective enterprise auditor.

This course will prepare students to:

- Apply risk-based decision making to the task of auditing enterprise security

- Understand the different types of controls (e.g., technical vs. non-technical) essential to performing a successful audit
- Conduct a proper risk assessment of an enterprise to identify vulnerabilities and develop audit priorities
- Establish a well-secured baseline for computers and networks as a standard to conduct audit against
- Perform cloud environment audits using automated tools and a repeatable process
- Audit virtualization hosts and container environments to ensure properly deployment and configuration
- Utilize vulnerability assessment tools effectively to provide management with the continuous remediation information necessary to make informed decisions about risk and resources
- Audit a web application's configuration, authentication, and session management to identify vulnerabilities attackers can exploit
- Utilize automated tools to audit Windows and Linux systems
- Audit Active Directory Domains

ISE 5800 IT Security Project Management (3 credits)

SANS class: MGT525, Managing Cybersecurity Initiatives and Effective Communication
Assessment: GIAC Certified Project Manager (GCPM)
3 Credit Hours

This course is focused on delivering bottom line value from security initiatives while following modern adaptive, agile, iterative, and predictive development approaches and leveraging the benefits of increased effective organizational communication. During this class students learn how to improve project planning methodology and project task scheduling to get the most out of critical IT resources. We utilize cyber security project case studies to increase practical understanding of real-world issues. MGT525 follows the basic methodologies and principles from the updated PMBOK® Guide, also providing specific implementation techniques for success. Throughout the 5 sections, all aspects of leading security initiatives - from project business justification analysis, selecting the appropriate development approach that fits your stakeholder and organizational structure using predictive, adaptive, and hybrid implementations tailored to drive value - are covered. We focus on planning for and managing cost, time, quality, and risk while your project is active, to completing, closing, and documenting as your project finishes. A copy of the PMBOK® Guide Seventh edition is provided to all participants. Students can reference the PMBOK® Guide and use course material along with the knowledge gained in class to prepare for the GIAC Certified Project Manager Exam (GCPM) and earn PDUs/CPEs to maintain the Project Management Professional (PMP)® and other professional credentials.

Project management methodologies and frameworks are highlighted that can be applied across any product life cycle, in any industry. Although our primary focus is the application of security initiatives, our approach is transferable to any projects that create and maintain services as well as general product development. We cover in-depth how cost, time, quality, risk, and compliance aspects affect the services we provide to others. We will also address practical human resource management as well as effective communication and conflict resolution. You will learn specific tools to bridge the communications gap between managers and technical staff.

This course will prepare students to:

- Understand predictive / waterfall, adaptive / agile development approaches and how they interact with product and project life cycles.
- Learn how to use and implement lean / agile tools, complexity models, root cause analysis
- Recognize the top failure mechanisms related to security projects, so that your projects can avoid common pitfalls
- Create a project charter which increases stakeholder engagement
- Document project requirements and create requirements traceability matrix to track changes throughout the project lifecycle
- Clearly define the scope of a project in terms of cost, schedule, and technical deliverables
- Develop a project schedule, including critical path tasks and milestones
- Cultivate user stories to drive adaptive sprint cycles
- Create accurate project cost and time estimates
- Develop planned and earned value metrics for your project deliverables and automate reporting functions
- Effectively manage conflict situations and build communication skills with your project team
- Analyze project risks in terms of probability and impact, assign triggers and risk response responsibilities
- Create project earned value baselines and project forecasts based on actual performance

Communicate effectively with stakeholders, technical staff, and management teams

5. **Discuss how general education requirements will be met, if applicable.**
   As a post-baccalaureate certificate program, the Software Supply Chain Security program does not include general education requirements.

6. **Identify any specialized accreditation or graduate certification requirements for this program and its students.**
   Each student who earns a Software Supply Chain Security post-baccalaureate certificate will have achieved certification in four areas of cybersecurity using Global Information Assurance Certifications (GIAC).

7. **If contracting with another institution or non-collegiate organization, provide a copy of the written contract.**
   Under a formal Memorandum of Understanding (MOU), STI outsources to SANS (STI's parent organization) many of the operational and administrative functions required to support operations, including establishment of most of our learning environments (physical and virtual), financial transactions, accounting, technology, and other administrative support services. Using this mechanism, STI benefits from SANS's economies of scale and transforms typically high-fixed-cost elements into manageable, smaller variable costs. STI also benefits from its relationship with Global Information Assurance Certification (GIAC), a sister company also owned by SANS. GIAC was established in 1999 to develop and offer exams and certifications that validate whether an individual has gained sufficient competency or mastery

of the complex topics taught in SANS courses, and most technical STI courses require students to pass a GIAC certification exam. GIAC exams are the product of broad-based job task analyses that incorporate feedback from hundreds of industry participants. Exam questions and answers and scoring patterns are reviewed and assessed by a PhD in psychometrics. Many of these certification exams have been designed with such a degree of quality that they are, themselves, certified by the American National Standards Institute (ANSI). Thus, learning in STI's Software Supply Chain Security courses is validated not by exams created by individual faculty members, but by assessments created by a highly specialized exam creation and testing organization that also keeps these exams current with changing professional requirements over time.

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

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

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

STI has a demonstrated record of completeness and transparency in all its academic programs and commits to maintaining a very high level of clarity, thoroughness, and timely information on the curriculum, course and degree requirements, nature of faculty/student interaction, assumptions about technology competence and skills, technical equipment requirements, learning management system, availability of academic support services and financial aid resources, and costs and payment policies. You can see evidence of the clarity and completeness of STI's existing graduate programs at
Graduate admissions: https://www.sans.edu/admissions/graduate/,
Master's degree academic page: https://www.sans.edu/cyber-security-programs/masters-degree/, and
Graduate certificate academic page: https://www.sans.edu/graduate-certificates/.

9. **Provide assurance and any appropriate evidence that advertising, recruiting, and admissions materials will clearly and accurately represent the proposed program and the services available.**

We commit to provide only clear and accurate information in our advertising, recruiting, and admissions material. Evidence of the clarity of our advertising and recruiting and admissions information for graduate studies may be found at: https://www.sans.edu/admissions/graduate/.

H. Articulation

As a technically focused post-baccalaureate certificate program and the only of its type in Maryland, 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 Software Supply Chain Security 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.

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 the people 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.

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.

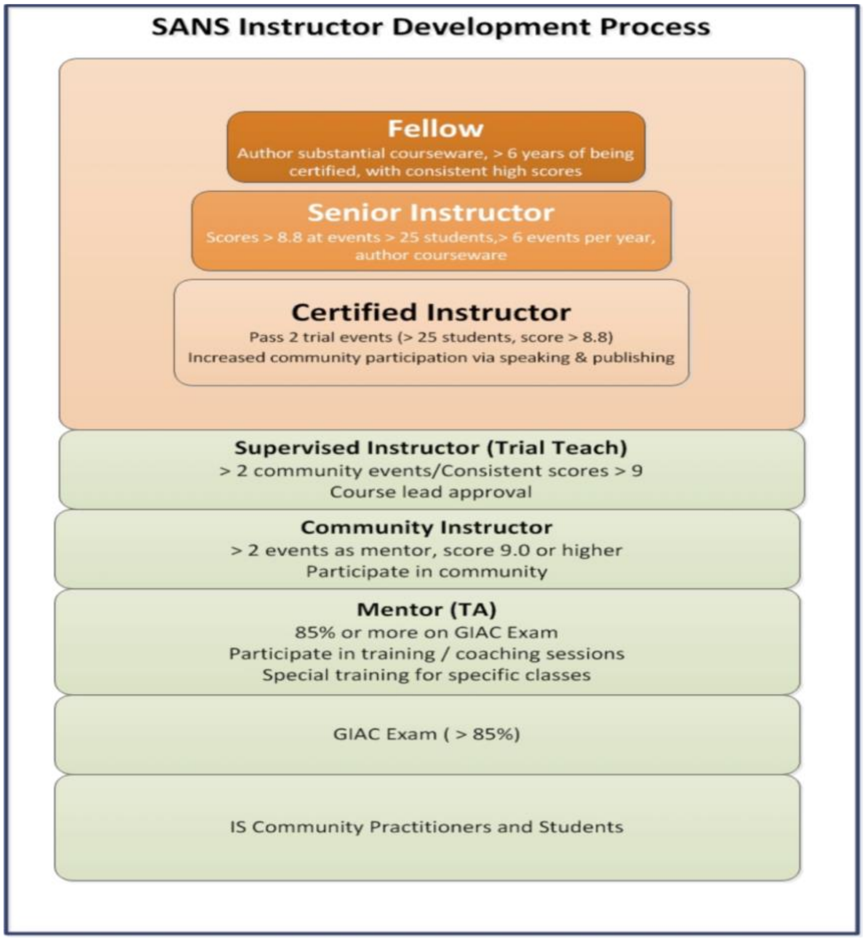
Only after completing these four steps would an individual be eligible to be a SANS Certified Instructor and potentially be appointed to the STI faculty.

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

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

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

Figure 1. SANS Instructor Development and Assessment Process


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

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.

A summary list of these Software Supply Chain Security post-baccalaureate 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 storytelling into their classroom presentation style.

LMS and Distance Education Training for Faculty:

The Software Supply Chain Security post-baccalaureate 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, Live Online, 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, Live Online 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 distinguish 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/.
- 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 Software Supply Chain Security students each year with a cumulative capacity of more than 40,000 students.

Additionally, the Software Supply Chain Security 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)	228000	364800	376200	421800	421800
a. Number of F/T Students	20	32	33	37	37
b. Annual Tuition/Fee Rate	11400	11400	11400	11400	11400
c. Total F/T Revenue (a x b)	228000	364800	376200	421800	421800
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)	228000	364800	376200	421800	421800

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 post-baccalaureate certificate students per month, with approximately one-quarter typically going into our Incident Response program, another quarter into our Penetration Testing program, on fifth in the Cloud Security program, and the remaining admits split into the Cyber Defense, Cyber Core, Cybersecurity Management, Purple Team Operations, and Industrial Control systems programs. Thus, it is our more narrowly focused post-baccalaureate 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 post-baccalaureate certificate program to eventually be nearly on par with our two largest certificate programs.

   The tuition projection for Year 1 assumes the Software Supply Chain Security program admits 20 full-time students during the year, each of whom pay $5,700 per course. Currently, our graduate students complete an average of 2 courses per year, supporting an effective annual tuition of $11,400 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 post-baccalaureate 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 post-baccalaureate 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
Software Supply Chain Security 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 Software Supply Chain Security 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, Software Supply Chain Security 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 Software Supply Chain Security 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 post-baccalaureate 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 post-baccalaureate 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 Software Supply Chain Security 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 Software Supply Chain Security 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 Program** (as 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 Live Online 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 Software Supply Chain Security 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 post-baccalaureate 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 (as outlined in COMAR 13B.02.03.05).

COMAR 13B.02.03.05 calls for higher education institutions to focus on equal opportunity concerns and on the expansion of educational opportunities and choices for minority and educationally disadvantaged students. The SANS Technology Institute collaborates with our SANS CyberTalent partner (https://www.sans.org/cybertalent/) to provide exactly those opportunities for Maryland residents. CyberTalent provides not only the Maryland Cyber Workforce Academy (https://www.sans.org/cybertalent/cyber-workforce-academy-maryland), but also routinely provides Diversity Cyber Academies that are open to Maryland residents. These Diversity Academies are intensive, accelerated training programs that provide SANS world class training and GIAC certifications to quickly and effectively launch careers in cybersecurity. SANS CyberTalent Immersion Academies are 100% scholarship-based and no cost to participants. Upon graduating from a Diversity Academy and gaining employment in the cybersecurity field, where employers routinely provide extensive training and education support, the SANS Technology Institute ensures that all Diversity Academy graduates are aware that their prior immersion training is potentially eligible for waiver into any of our undergraduate or graduate programs, allowing the student to enter with advanced standing and reduced program cost, and that we work with a wide array of employers to ensure that continuing education is available at no cost to the employee whenever possible.

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

Not applicable.

P. Adequacy of Distance Education Programs (outlined in COMAR 13B.02.03.22).

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

Contents

General Information

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 lcgitimate 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,	Generalized STI marketing campaigns are made

	graphic editing, and industry expertise required to allow for the execution of STI recruitment campaigns	operational via the availability of a centralized SANS marketing staff

Information Technology

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

Technical Course Maintenance & Presentation

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

Educational Residency

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

Service Constraints

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

Terms of Agreement

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

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

Periodic Quality Reviews

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

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

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

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

Service Level Maintenance

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

Issue Resolution

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

Payment Terms and Conditions

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

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

Agreed to on behalf of STI:

Eric A. Patterson

Provost

SANS Technology Institute

Date:

Agreed to on behalf of SANS:

Peggy Logue

Chief Financial Officer

SANS Institute

3/17/23

Date:

Appendix A:

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

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

SANS Technology Institute-GIAC Memorandum of Understanding

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

Contents

General Information

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 have obtained a knowledge base in information security to GIAC standards.

Mission

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

Scope

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

Hours of Operations

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

Service Expectations

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

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

Service Constraints

- ***Conformance Requirements -*** ANAB (ANSI National Accreditation Board) 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 June 1, 2023 - 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 Provost and the General Manager 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 $400 each time a student pays for a GIAC exam, to include the GSE Entrance Exam, as part of their program of studies.
- STI will pay GIAC $150 each time a student pays for a practitioner exam, to include GFACT and SSAP.
- If **ACSCFT** registration code is used, no MOU fee is charged.

Agreed to on behalf of STI:

Eric A. Patterson
Provost
SANS Technology Institute

09 February 2023
Date

Agreed to on behalf of GIAC:

Jeremy Rabson
General Manager
GIAC

February 9th, 2023
Date

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

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

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

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

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

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

(a) Curriculum and instruction

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

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

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

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

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

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

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

Table A4.1. Comparison of GIAC Exam Score Performance via Live and OnDemand Modalities, 2014–2017

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

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

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

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

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

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

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

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

STI faculty members design all distance learning programs.

(b) Role and mission

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

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

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

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

(c) Faculty support

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

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

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

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

Instructor Guidelines for SANS Simulcast Classes

What to Expect

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

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

Advance Planning

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

Audio Tips

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

Starting Class

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

Teaching Tips

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

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

Suggested Best Practices

Jason Fossen (SANS Senior Instructor):

o Each day I used a second laptop to log onto vLive as an attendee so that I could see how fast my application sharing window was updating its screen.

◊ It was also useful for checking the sound, video, and file-sharing features.

◊ I granted my other account moderator status so that, in case my primary laptop had an issue, I could switch over to the secondary and continue teaching.

- 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 (SANS Senior Instructor):

- 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.

(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/.
- The SANS Internet Storm Center Archives contain contemporaneous analyses of new attacks that are discovered on the Internet. The archives constitute an extraordinary research asset because of the depth of the analysis and the currency of the topics covered. They also provide SANS students with access to raw data, summaries, and query facilities to analyze malicious Internet traffic records. This is a rich data source for advanced security research projects that analyze attack patterns and how fast worms spread through the Internet.
- SANS Web Briefings held several times a month feature SANS faculty and other security experts providing up-to-date web briefings for SANS alumni on new threats seen at the Internet Storm Center, new technologies that are emerging, and analysis of security trends.

(e) Students and student services

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

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

- Course and degree requirements are posted online in the STI Graduate Course Catalog.

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

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

- Technical equipment requirements are posted with individual courses on the SANS course website. For example, for ISE 6650: Cloud Security and DevSecOps Automation, the corresponding course site at SANS (https://www.sans.org/cyber-security-courses/cloud-security-devsecops-automation/) provides detailed technical requirements as well as a tech support contact to help students ensure they have the right equipment and software versions.

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

- The availability of academic support services and financial aid resources is posted at https://www.sans.edu/students/services, and on page 15 of the Student Handbook at https://www.sans.edu/downloads/sti-student-handbook.pdf

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

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

With STI students taking approximately half of their credits through distance learning, the overall satisfaction with student services may be considered a reliable surrogate for effectiveness of distance learning student services. Evidence from student surveys indicates that measures of overall student satisfaction are high (above 90%)/. Quantified measures of specific sub-processes with student management were also high, with about 90% of respondents saying they were "Somewhat Satisfied" and "Very Satisfied" for each of the operational elements (Table A4.2).

Table A4.2. Student Satisfaction with Student Management as Reported in the 2016 Student Experience Survey

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

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

Our Software Supply Chain Security students will be lower division students, likely at least 19 years old, and sufficiently well versed in information technology to have scored sufficiently high on the cyber aptitude test and simulator gain acceptance. Thus, they have the needed background, knowledge, and technical skills to use the distance learning modalities.

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

Advertising, recruiting, and admissions materials for Software Supply Chain Security 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 Software Supply Chain Security program. Further, because graduate programs are core to our mission and were 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 Software Supply Chain Security 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 Software Supply Chain Security program will be measured by grades on the internationally standardized GIAC exams for each area of security. We compare these scores in distance and in-person learning modalities. As shown in Table A4.3, the GIAC test scores in distance learning are essentially identical to scores of students who used live, in-person residential training programs:

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

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

We will continue to monitor GIAC scores in the Software Supply Chain Security program, by delivery modality.

Appendix 3. Summary Listing of Software Supply Chain Security post-baccalaureate certificate Faculty

Last Name	First Name	Highest Degree	Highest Degree Field	Academic Rank	Title	Status	Courses Taught
Johnson	Eric	Master’s	Information Assurance	Senior Instructor	Professor	Part Time	ISE 6650 ISE 6612
Kim	Frank	Master’s	MBA	Faculty Fellow	Professor	Full Time	ISE 6650
Nicholson	Ryan	Master’s	Cybersecurity and Information Assurance	Instructor	Instructor	Part Time	ISE 6610
Baggett	Mark	Master’s	Information Security Engineering	Senior Instructor	Professor	Part Time	ISE 6350
Ullrich	Johannes	PhD	Physics	Faculty Fellow	Dean of Research	Full Time	ISE 6615
Conrad	Eric	Master’s	Information Security Engineering	Faculty Fellow	Professor	Part Time	ISE 6315
Frost	Moses			Senior Instructor	Professor	Part Time	ISE 6630
Frisk	Jeff	Bachelor’s	Engineering	Instructor	Instructor	Part Time	ISE 5800
Risenhoover	Clay	Master’s	Computer Science	Principal Instructor	Instructor	Part Time	ISE 6715