SANS Technology Institute

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

March 1, 2026

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

Dear Dr. Rai,

The SANS Technology Institute is pleased to submit the attached proposal to create a new Post-Baccalaureate Certificate in Digital Forensics. This submission follows MHEC's recent review of the Letter of Intent (LOI) from SANS Technology Institute for a Post Baccalaureate Certificate (P.B.C.) in Digital Forensics, submitted on January 15, 2026 (ref: LOI050).

This post-baccalaureate certificate will provide students with the knowledge and training necessary to collect, preserve, analyze, and communicate digital evidence in support of criminal, civil, and cybersecurity investigations across government, military, and private-sector environments.

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

Ed Skoudis
President
SANS Technology Institute

Office Use Only: PP#

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

Institution Submitting Proposal	SANS Technology Institute

Each action below requires a separate proposal and cover sheet.

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

Payment Submitted: (●) Yes ( ) No

Payment Type: ( ) R*STARS # 190774 (●) Check # 190774

Payment Amount: $850

Date Submitted: 12/22/25

Department Proposing Program	SANS Technology Institute	
Degree Level and Degree Type	Post-baccalaureate Certificate	
Title of Proposed Program	Digital Forensics	
Total Number of Credits	12	
Suggested Codes	HEGIS: 5199	CIP: 11.1003
Program Modality	( ) On-campus ( ) Distance Education (fully online) (●) Both	
Program Resources	(●) Using Existing Resources ( ) Requiring New Resources	
Projected Implementation Date (must be 60 days from proposal submisison as per COMAR 13B.02.03.03)	( ) Fall ( ) Spring (●) Summer	Year: 2026
Provide Link to Most Recent Academic Catalog	URL: https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltbeae8a35690b977d/graduate-course-catalog.pdf	
Preferred Contact for this Proposal	Name: Eva Dring	
	Title: Director of Academic Affairs	
	Phone: (301) 371-2142	
	Email: edring@sans.edu	
President/Chief Executive	Type Name: Ed Skoudis	
	Signature: [signature]	Date: 12/22/2025
	Date of Approval/Endorsement by Governing Board:	12/22/2025

Revised 1/2021

Proposal for a New Academic Program:

Post-baccalaureate Certificate in Digital Forensics

SANS Technology Institute

March 1, 2026

Post-Baccalaureate Certificate in Digital Forensics

SANS Technology Institute

Table of Contents

A. Centrality to Institutional Mission Statement and Planning Priorities

1. Program Description

The SANS Technology Institute (SANS.edu) proposes to launch a Post-Baccalaureate Certificate in Digital Forensics, a 12-credit graduate-level certificate designed to prepare working professionals to collect, preserve, analyze, and communicate digital evidence across a wide range of investigative environments.

This program responds directly to growing workforce needs in law enforcement, government, military, and private-sector DFIR (Digital Forensics and Incident Response) operations. Its curriculum provides students with hands-on mastery of host forensics, evidence acquisition, and mobile device forensics – three core pillars of modern digital investigations.

Students will complete three required core courses:

- **ISE 6498 – Digital Acquisition and Rapid Triage**
  Certification: GBFA – GIAC Battlefield Forensics and Acquisition

- **ISE 6500 – Windows Forensic Analysis**
  Certification: GCFE – GIAC Certified Forensic Examiner

- **ISE 6585 – Smartphone Forensic Analysis In-Depth**
  Certification: GASF – GIAC Advanced Smartphone Forensics

Students choose one elective from a curated list of Digital Forensics and Incident Response-aligned options. All courses are aligned to a GIAC certification exam, which serves as the validated assessment of student mastery.

The program fills a clearly defined need for a dedicated Digital Forensics academic pathway – distinct from the college's existing Incident Response graduate certificate – and enables students to stack credentials while avoiding unnecessary course overlap.

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

The mission of the SANS Technology Institute (SANS.edu) is to develop technically skilled professionals and leaders who strengthen global information security. This program directly supports that mission by addressing the increasing need for forensic examiners

capable of handling the surge in digital evidence across criminal investigations, cyber incidents, and enterprise risk events.

By providing a specialized pathway for forensic investigators, this program:

- contributes to SANS.edu's core strategic goal of expanding the pipeline of cybersecurity professionals;
- leverages the college's strengths in delivering hands-on, practitioner-led education;
- meets employer expectations for validated, job-ready forensic competencies;
- expands the Institute's portfolio of graduate certificates in high-demand cybersecurity subfields.

This certificate uses the same faculty, instructional systems, and delivery modalities (In-person, Live Online, and OnDemand) already supporting SANS.edu's accredited programs.

3. Funding for the Program

The program will be fully funded through tuition revenue. SANS.edu's strong financial position, growing enrollment, and scalable instructional model ensure that the program can be supported through its first five years and beyond.

No new faculty hires are required. Existing digital forensics expert instructors already teach the proposed courses across modality formats. Administrative and operational support will be covered by existing staff and scalable support agreements with the SANS Institute.

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

SANS.edu is deeply committed to the long-term success of this program. The Digital Forensics domain is integral to national security, crime prevention, and enterprise cyber resilience. The SANS FOR courses used in this certificate are regularly updated and among the most in-demand offerings in the global SANS curriculum.

SANS.edu will maintain course availability across modalities, support ongoing GIAC exam updates, provide robust academic advising and technical support, and ensure enrolled students can complete the program even if future curricular updates occur.

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

1. Critical Need for the Program

Nearly every modern investigation – criminal, civil, corporate, or national security-related – now involves digital evidence. A 2025 review of SANS.edu's Incident Response (IR) certificate found an increasing divide between students seeking IR-focused skills and those requiring deeper acquisition and forensic analysis capabilities.

Key drivers of demand include:

- rapid increase in digital evidence volume across all types of crime;
- chronic shortages of forensic examiners in law enforcement and federal agencies;
- accelerated adoption of cloud, mobile, and SaaS platforms;
- increased sophistication of adversary tradecraft;
- growth of enterprise DFIR teams with specialized forensic roles.

This program creates a dedicated, validated pathway to develop forensic examiners capable of supporting investigations at all levels.

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

The proposed program supports multiple priorities in the 2022 State Plan:

- **Priority 5: High-Quality Postsecondary Education**
  Provides rigorous, validated, hands-on education aligned to GIAC certification.

- **Priority 6: Improve Timely Program Completion**
  Options for fully online and asynchronous delivery eliminate geographic and scheduling barriers.

- **Priority 7: Lifelong Learning and Workforce Mobility**
  Increases stackable credentials for working professionals seeking advancement.

- **Priority 8: Innovation and Risk-Taking**
  Addresses emerging forensic challenges including cloud, mobile devices, and encrypted platforms.

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

1. Institutional Demand

Digital forensic investigation functions are embedded within federal and defense operations across Maryland.

The U.S. Department of Defense operates the DoD Cyber Crime Center (DC3), located in Linthicum, Maryland, which provides digital and multimedia forensic services in support of national security missions[1]. DC3's mandate includes forensic analysis, investigative support, and digital evidence examination across defense and law enforcement environments.

Maryland's geographic concentration of federal agencies, defense contractors, intelligence operations, and critical infrastructure organizations contributes to sustained regional demand for digital forensic practitioners capable of conducting defensible evidence acquisition and analysis in investigative and operational settings.

In its LOI response, the Commission referenced statewide graduate production data indicating that Maryland institutions collectively produce more than 6,000 graduates annually in programs leading to occupations such as Computer and Information Systems Managers, Computer Systems Analysts, Computer Network Architects, and Database Administrators, compared with approximately 3,000 annual openings across those four occupations. While this macro-level comparison is informative, it aggregates broad computing and IT disciplines and does not isolate the labor market specific to digital forensic practitioners.

The proposed Post-Baccalaureate Certificate in Digital Forensics does not prepare students for general IT management, systems administration, database administration, or network architecture roles. Rather, it prepares practitioners for highly specialized investigative functions requiring forensic acquisition, artifact reconstruction, evidentiary documentation, and legally defensible analytical procedures. As such, general computing graduate counts do not serve as a proxy for supply in the digital forensic workforce segment.

The Workforce Analysis cited in the LOI response aggregates graduates across multiple broad occupational categories that are not functionally interchangeable with digital forensic investigative roles. A graduate prepared for database administration, network architecture, or IT management does not, by virtue of degree classification alone, possess competencies in forensic acquisition, artifact-level behavioral reconstruction, evidentiary

[1] DoD Cyber Crime Center: https://www.dc3.mil/

chain-of-custody, or legal documentation. Therefore, surplus production in general computing disciplines cannot be interpreted as surplus production in forensic investigative specialization.

2. National Labor Market Indicators

The U.S. Bureau of Labor Statistics projects 32% employment growth (2022–2032) for Information Security Analysts – substantially faster than the national average[2].

While this occupational classification aggregates multiple cybersecurity functions, digital forensic and incident response roles are included within this category.

Importantly, digital forensics functions represent a specialized subset of cybersecurity employment that is not evenly supplied by general cybersecurity degree programs. Many bachelor's programs categorized under cybersecurity or computer science emphasize governance, compliance, policy, or general defensive operations rather than evidentiary forensic investigation.

3. Maryland Cybersecurity Workforce Data (CyberSeek)

State-level workforce analytics further confirm sustained demand.

CyberSeek, a nationally recognized cybersecurity workforce data platform supported by NIST, CompTIA, and Lightcast[3] reports the following current Maryland cybersecurity labor metrics:

- 27,050 total online cybersecurity job openings
- 65,282 employed cybersecurity workers
- Supply vs. Demand Ratio: 73%

A 73% ratio indicates that Maryland has approximately 73 available cybersecurity workers for every 100 job postings, reflecting a documented labor shortfall.

Within the NICE Cybersecurity Workforce Framework categorization, Maryland reports 1,243 job openings in the "Investigation" category, defined as conducting cybersecurity and cybercrime investigations including the collection, management, and analysis of digital evidence. This category most directly aligns with digital forensic examiner and investigative roles. This category is distinct from the broader managerial and analytical

[2] BLS Occupational Outlook Handbook: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
[3] CyberSeek Heat Map: https://www.cyberseek.org/heatmap.html

occupations referenced in the LOI response and provides a more precise measure of demand for forensic capabilities.

4. Digital Forensics as a Specialized Discipline

Modern investigative practice increasingly relies on mobile, endpoint, and cloud-based evidence sources.

Federal technical guidance confirms digital forensics as a distinct and specialized discipline:

- NIST Special Publication 800-101 Rev. 1 formally defines mobile device forensics as a specialized area within digital investigations[4].
- CISA guidance emphasizes cloud log collection and forensic analysis as essential components of investigative response[5].
- The Verizon 2024 Data Breach Investigations Report documents that incident response investigations rely heavily on endpoint artifacts, log analysis, and evidence reconstruction requiring forensic acquisition capabilities[6].

In addition, federal civil litigation rules explicitly recognize electronically stored information (ESI) as discoverable evidence, reinforcing the need for defensible digital forensic preservation and analysis[7].

Cyber insurance regulatory frameworks likewise identify forensic investigation as a core component of breach response obligations[8].

Collectively, these authoritative sources demonstrate that digital forensic competencies are central to modern cybersecurity operations.

5. Certification Demand and Advanced Workforce Specialization

CyberSeek certification analytics for Maryland further illustrate employer demand for advanced cybersecurity credentials.

---

[4] NIST SP 800-101 Rev. 1: https://csrc.nist.gov/pubs/sp/800/101/r1/final
[5] CISA Cloud Logging Guidance: https://www.cisa.gov/resources-tools/resources/microsoft-expanded-cloud-logs-implementation-playbook
[6] Verizon DBIR: https://www.verizon.com/business/resources/reports/dbir/
[7] Federal Rules of Civil Procedure Rule 34: https://www.law.cornell.edu/rules/frcp/rule_34
[8] National Association of Insurance Commissioners – Cybersecurity: https://content.naic.org/cipr-topics/cybersecurity

Current Maryland job postings requesting certification include:

- GIAC: 2,492 postings
- CISSP: 4,057 postings
- CompTIA Security+: 5,919 postings
- CISM: 1,502 postings
- CISA: 1,407 postings

Maryland's estimated certification holders include:

- GIAC: 3,984 holders
- CISSP: 7,337 holders
- CompTIA Security+: 28,959 holders
- CISM: 1,888 holders
- CISA: 1,920 holders

The ratio of GIAC holders (3,984) to job postings requesting GIAC (2,492) reflects one of the tightest supply-demand alignments among listed certifications, indicating sustained employer recognition of GIAC as an advanced, role-aligned credential.

Unlike broad entry-level certifications, GIAC certifications are closely associated with practitioner-level cybersecurity functions including digital forensics, incident response, and investigative analysis. The comparatively limited number of GIAC holders relative to employer demand reinforces the need for specialized graduate-level preparation aligned with externally validated certification standards.

The proposed certificate is designed to prepare students for roles such as:

- Digital Forensic Analyst
- Cybercrime Investigator
- Incident Response Analyst (forensics-focused)
- Mobile Device Examiner
- DFIR Consultant
- eDiscovery Specialist

Employers frequently specify GIAC certifications – including **GBFA, GCFE, GASF** – as preferred or required qualifications for these roles, directly aligning with this program[9].

[9] Examples of such job postings include:

Host Forensics Analyst, NewGen Technologies – https://lensa.com/job-v1/newgen-technologies-maryland/arlington-va/host-forensics-analyst/2fd431cd18b1c50668bd6b2c4f7d25b7
Senior Forensics Specialist – https://www.celeritasinc.com/job/senior-forensics-specialist-la-hybrid-

Unlike entry-level certifications, GIAC credentials aligned to forensic roles require demonstrated mastery of artifact-level analysis, evidentiary handling, and applied investigative workflows. The relatively narrow pool of GIAC holders compared to broader certifications such as Security+ indicates that advanced forensic competencies are not widely distributed among general cybersecurity graduates. This further supports the conclusion that specialized forensic preparation is not oversupplied in Maryland.

6. Supply Considerations

Maryland institutions graduate substantial numbers of students in general cybersecurity and information technology disciplines. However, general cybersecurity curricula typically emphasize governance, policy, risk management, or broad security operations.

Digital forensic roles require distinct technical competencies, including:

- Forensically sound evidence acquisition and chain-of-custody procedures
- Host, mobile, and cloud artifact reconstruction
- Cross-platform timeline correlation
- Documentation suitable for investigative and legal proceedings.

These competencies are not typically embedded as required, externally validated program elements within general cybersecurity programs.

Accordingly, while Maryland produces significant numbers of cybersecurity graduates, quantifiable workforce data demonstrate continued statewide labor shortages and documented employer demand for specialized investigative and GIAC-aligned competencies. The proposed Post-Baccalaureate Certificate in Digital Forensics expands Maryland's capacity to develop advanced forensic practitioners capable of supporting federal, state, military, enterprise, and legal investigative environments.

To further contextualize statewide supply, MHEC identified four Maryland post-baccalaureate certificates specifically related to digital or computer forensics. Even assuming an average cohort size of approximately 20–25 graduates annually per program, statewide production capacity for specialized forensic certificate holders would likely total fewer than 100 graduates per year. This estimated production level is modest relative to the documented 1,243 current Investigation-category job openings reported by CyberSeek and does not indicate systemic oversupply. This figure is materially distinct from the 6,000 annual graduates across all computing disciplines cited in the Workforce Analysis. Moreover, the proposed SANS.edu certificate is designed for mid-career professionals who are frequently already employed in cybersecurity, defense, law enforcement, or enterprise

---

Cyber Defense Forensics Analyst, Booz Allen – https://careers.boozallen.com/jobs/JobDetail/San-Antonio-Cyber-Defense-Forensics-Analyst-R0229762/117979?utm

environments. The program therefore deepens specialization within the existing workforce rather than expanding entry-level supply. As a result, it does not materially contribute to generalized workforce saturation concerns identified in the LOI response.

D. Reasonableness of Program Duplication

1. Similar Programs in the State

Digital Forensics, Computer Forensics and Cyber Investigation

A review of programs listed in the Maryland Higher Education Commission (MHEC) inventory shows four existing post-baccalaureate certificates related to digital or computer forensics in the state:

- **Capitol Technology University – Post-Baccalaureate Certificate in Digital Forensics & Incident Handling**
  Focuses on foundational concepts in forensic investigation and incident handling within information assurance contexts, with coursework emphasizing introductory digital evidence processes and basic incident-response techniques.

- **Stevenson University – Post-Baccalaureate Certificate in Digital Forensics**
  Provides a general introduction to digital forensics methodology, including evidence acquisition and analysis. The program is geared toward entry-level or cross-training professionals and is structured around broad survey-level competencies.

- **Towson University – Post-Baccalaureate Certificate in Computer Forensics**
  Offers a mixture of online and in-person courses preparing students for roles involving initial digital-evidence handling and basic forensic examination. The curriculum is situated within Towson's applied information technology programs and emphasizes computer-forensics fundamentals.

- **University of Maryland Global Campus (UMGC) – Graduate Certificate in Digital Forensics & Cyber Investigation**
  A 12-credit online certificate covering foundational digital-forensics concepts, including securing and validating evidence, recovering artifacts from common platforms, and preparing digital findings within investigative or legal processes.

These programs contribute meaningfully to Maryland's cybersecurity and digital forensics education ecosystem and provide important entry points into the field. However, they differ materially in scope, depth, assessment structure, and intended audience from the proposed SANS Technology Institute Post-Baccalaureate Certificate in Digital Forensics. While these programs share topical relevance to digital forensics, none offers the specialized, advanced, practitioner-level digital forensics training delivered through the proposed SANS Technology Institute Graduate Certificate.

The distinctions between the proposed program and existing Maryland certificates may be summarized across four measurable dimensions:

- **Assessment Structure**
  - Existing Programs: Course-level assessments developed and administered internally.
  - Proposed Program: Academic credit contingent upon passing independent, ANSI-accredited GIAC certification examinations aligned to each core course.

- **External Validation of Learning Outcomes**
  - Existing Programs: No required third-party psychometrically validated examination required for program completion.
  - Proposed Program: Each required course maps directly to a GIAC certification (GBFA, GCFE, GASF), developed through formal job-task analysis and reviewed under ANSI accreditation standards.

- **Technical Scope and Depth**
  - Existing Programs: Provide foundational or survey-level exposure to digital forensic concepts.
  - Proposed Program: Requires demonstrated proficiency in rapid triage workflows, full-file-system mobile extraction, artifact-level behavioral reconstruction, cross-platform timeline correlation, and evidentiary documentation suitable for legal proceedings.

- **Intended Audience**
  - Existing Programs: Serve entry-level learners or general cybersecurity cross-training.
  - Proposed Program: Designed specifically for mid-career practitioners operating in federal, military, intelligence, law enforcement, and enterprise investigative environments.

Given these distinctions, the proposed program fills a clear unmet need in Maryland for an advanced, graduate-level technical forensics credential that supports modern investigative operations. Although related certificates exist, none provides the depth, specialization, certification alignment, or practitioner-oriented curriculum offered by this program. Therefore, the program is not unreasonably duplicative under COMAR 13B.02.03.09(C).

MHEC Academic Program Inventory (API) Review

A review of the Commission's Academic Program Inventory (API) identified additional post-baccalaureate and graduate-level programs classified under CIP Code 11.1003 – Computer and Information Systems Security – that may be broadly related to the proposed Post-Baccalaureate Certificate in Digital Forensics. These programs include:

- **Towson University** – Information Security & Assurance
- **University of Maryland, Baltimore County** – Cybersecurity Informatics
- **University of Maryland Global Campus** – Cybersecurity Technology
- **University of Maryland Global Campus** – Foundations of Cybersecurity
- **University of Maryland Global Campus** – Cybersecurity Management & Policy
- **University of Maryland Global Campus** – Cyber Operations
- **Morgan State University** – Cyber Security
- **Capitol Technology University** – Health Care Systems Security
- **Capitol Technology University** – Information Assurance Administration
- **Capitol Technology University** – Security Management
- **Capitol Technology University** – Network Protection
- **Capitol Technology University** – Secure Mobile Technology
- **Capitol Technology University** – Secure Software Development
- **Capitol Technology University** – Secure Cloud Computing
- **Hood College** – Cybersecurity
- **Loyola University Maryland** – Cyber Security
- **Mount St. Mary's University** – Risk Management & Cybersecurity for Professionals

While programs classified under CIP 11.1003 contribute to Maryland's overall cybersecurity workforce pipeline, they predominantly emphasize governance, risk management, policy, cyber operations, or general security engineering. They do not require advanced digital forensic acquisition, artifact reconstruction, or external ANSI-accredited certification validation as a condition of completion. As such, CIP classification similarity does not equate to curricular or functional duplication.

The proposed SANS.edu Digital Forensics certificate is narrowly focused on practitioner-level forensic methodologies, including evidentiary acquisition, cross-platform artifact analysis, mobile device forensics, and externally validated competency through required ANSI-accredited GIAC certification examinations. It is designed for mid-career professionals seeking advanced forensic specialization rather than broad cybersecurity exposure.

Existing programs contribute meaningfully to Maryland's broader cybersecurity education landscape, but these programs do not duplicate the scope, depth, assessment structure, or intended outcomes of the proposed Digital Forensics certificate and therefore do not constitute unreasonable duplication under COMAR 13B.02.03.09(C).

2. Justification for the Proposed Program

Although related digital forensics certificates exist within Maryland, none offers a graduate-level, practitioner-focused program centered on advanced forensic acquisition,

artifact reconstruction, mobile device analysis, and externally validated competency assessment through ANSI-accredited certification examinations.

The proposed certificate should be understood not as an additional general cybersecurity offering, but as a post-baccalaureate specialization layered upon prior computing or cybersecurity education. It addresses advanced investigative competencies that are not typically embedded as required components within general cybersecurity degree pathways.

Maryland's unique concentration of federal investigative agencies, defense contractors, intelligence operations, and enterprise security teams creates a sustained demand for forensic examiners capable of:

- Conducting legally defensible evidence acquisition
- Performing advanced artifact and timeline reconstruction
- Analyzing mobile and cloud-based evidence sources
- Operating in complex investigative and national-security environments

These capabilities are operational in nature and directly aligned to investigative missions in national security, criminal justice, enterprise incident response, and civil litigation environments. The program therefore serves a specialized professional cohort rather than competing for the same student population as broad cybersecurity programs.

Existing programs primarily provide foundational exposure to digital forensics concepts. The proposed SANS.edu certificate addresses a distinct and higher level of specialization focused on operational forensic practice and validated technical competence.

Therefore, while related certificates are offered in the State, the scope, technical depth, externally validated assessment model, and intended mid-career practitioner audience of the proposed program are materially distinct. The requirement that students successfully complete ANSI-accredited GIAC certification examinations as a condition of earning academic credit represents a structural difference in program design and outcome validation. This external, psychometrically validated assessment requirement establishes a materially different academic model from programs relying solely on internally designed course assessments, and creates a distinct threshold of demonstrated professional competency. For these reasons, the proposed Post-Baccalaureate Certificate in Digital Forensics does not constitute unreasonable duplication under COMAR 13B.02.03.09(C).

As noted in the Commission's LOI response, MHEC encouraged exploration of potential collaboration with institutions offering related programs. SANS.edu remains open to dialogue with Maryland institutions where collaboration may advance workforce preparation or create complementary pathways. However, given the distinct scope, practitioner-focused design, and embedded certification assessment model of the proposed Digital Forensics certificate, the program is structured as a specialized graduate

credential rather than as a transfer or co-delivery pathway. Accordingly, formal program integration with existing certificates is not presently anticipated.

In summary, the proposed certificate addresses a specialized investigative workforce segment not captured by aggregate computing graduate data, operates at a distinct technical depth validated through ANSI-accredited external assessment, and targets mid-career practitioners rather than entry-level cybersecurity students. For these reasons, the program expands Maryland's forensic workforce capacity without duplicating existing offerings or contributing to generalized workforce oversupply.

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

No HBI in Maryland offers a Digital Forensics-focused graduate certificate. The program does not duplicate, compete with, or diminish high-demand programs at HBIs. Instead, it expands advanced-skills pathways for graduates of HBI undergraduate programs.

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

A review of programs offered at Maryland's four HBIs (Bowie State University, Coppin State University, Morgan State University, and the University of Maryland Eastern Shore) confirms that none offers a graduate or post-baccalaureate certificate in Digital Forensics or a closely comparable technical digital-forensics credential. Existing HBI offerings in cybersecurity or forensic investigation are either undergraduate, broad in focus, or oriented toward criminal-justice practice rather than advanced digital-evidence analysis.

Because the proposed program is:

- fully online,
- post-baccalaureate,
- designed for mid-career professionals with significant technical experience, and
- highly specialized in advanced digital-forensics practice,

it does not compete with, duplicate, or divert students from any HBI mission-related programs. The program therefore has no adverse impact on the identity, mission, or resource base of Maryland's Historically Black Institutions.

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

(Outlined in COMAR13B.02.03.10)

The curriculum for the Post-Baccalaureate Certificate in Digital Forensics is designed to ensure that students develop the applied forensic competencies required by law enforcement, military, intelligence, and private-sector incident response organizations. Its structure reflects industry-validated job-task analyses and is aligned to ANSI-accredited GIAC certification exams, which serve as rigorous assessments of student learning.

This section addresses all elements required by COMAR 13B.02.03.10, including the program's establishment, faculty oversight, educational objectives, learning outcomes, assessment methods, curriculum design, and program requirements.

1. Program Establishment and Faculty Oversight

The Digital Forensics certificate was established in response to:

- demonstrated workforce demand across Maryland and the nation;
- increasing volumes of digital evidence encountered in criminal, civil, and cyber investigations;
- increased student demand for advanced technical training in collection, preparation and analysis of such digital evidence, particularly in relation to smartphones, where there is an increasing divide between the quantity of available evidence and the volume of expert practitioners with the capability to analyze it;
- a 2025 review of STI's Incident Response certificate, which identified a clear need for a distinct but complementary Digital Forensics pathway focused on evidence acquisition and artifact analysis.

The program was designed collaboratively by the SANS Digital Forensics & Incident Response (DFIR) Curriculum Lead, senior SANS instructors, and SANS.edu's academic leadership. These faculty members are internationally recognized forensic experts with decades of investigative experience and leadership roles in federal law enforcement, the Department of Defense, and private-sector incident response.

Faculty responsibilities include:

- approving curriculum content and learning outcomes;
- ensuring alignment with emerging forensic techniques, tools, and real-world investigative practices;
- overseeing delivery quality across in-person, Live Online, and OnDemand modalities;

- maintaining academic integrity and program coherence.

This instructional oversight model is identical to that used for SANS.edu's existing accredited graduate programs. A summary list of program faculty is included in Section *I. Adequacy of Faculty Resources*.

2. Educational Objectives and Learning Outcomes

The program is designed to prepare graduates to perform technically rigorous digital forensic investigations with accuracy, defensibility, and investigative insight. Learning outcomes reflect recognized DFIR competencies and are directly mapped to GIAC certification objectives, and these objectives are common across all delivery modalities.

After completing the program, students will be able to:

1. Explain the role and scope of Digital Forensics within cybersecurity and investigative operations.
   - Describe how Digital Forensics supports timeline reconstruction, legal processes, and investigative decision-making.
   - Distinguish the applications of digital forensics across host-based investigations and other core investigative domains.

2. Collect, triage, preserve, and document digital evidence while maintaining evidentiary integrity.
   - Assess evidence volatility and prioritize acquisition based on time-to-evidence considerations, including rapid collection and triage workflows.
   - Apply appropriate preservation and documentation techniques to maintain a defensible chain of custody.
   - Acquire and prepare evidence from a range of platforms (e.g., Windows, macOS, iOS, virtual machines, cloud sources) to support investigative and legal requirements.

3. Conduct in-depth forensic analysis across diverse platforms to establish factual event timelines.
   - Analyze artifacts from Windows systems, mobile devices, and other supported platforms to identify and interpret key indicators of user and system activity.
   - Correlate artifacts across platforms to determine "ground truth" of system and user activity.

4. Evaluate and apply forensic tools and methodologies to ensure accurate, reliable results.

- Validate tool outputs and interpret artifacts with analytical rigor.
- Contextualize and corroborate findings across hosts and networks to support investigative reconstruction.

5. Demonstrate a comprehensive understanding of key forensic artifacts and their behaviors.
   - Identify persistent artifacts across platforms and understand how they contribute to accurate timeline creation.
   - Use artifact behavior to interpret user actions, system events, and adversary activity.

These outcomes reflect those most frequently requested in Digital Forensics job postings across Maryland and national agencies.

3. Assessment of Student Achievement and Documentation of Learning Outcomes

(a) Assessment of Student Learning

SANS.edu uses externally validated, ANSI-accredited GIAC certification exams as the primary method of assessing student achievement. Each required course maps directly to a GIAC certification:

- **ISE 6498** maps to **GBFA** (GIAC Battlefield Forensics and Acquisition)
- **ISE 6500** maps to **GCFE** (GIAC Certified Forensic Examiner)
- **ISE 6585** maps to **GASF** (GIAC Advanced Smartphone Forensics)
- One elective course with GIAC certification aligned to the chosen specialization

GIAC exams validate both theoretical understanding and the ability to perform hands-on forensic tasks under time constraints.

No student may earn academic credit for a course without passing the corresponding GIAC exam.

(b) Documentation of Student Achievement

SANS.edu documents student achievement through:

- GIAC exam results stored in secure academic records
- LMS-based tracking of lab completion and instructor interaction
- daily learner evaluations of course delivery

- annual program assessment reports
- five-year comprehensive program reviews conducted under SANS.edu's Learning Outcomes Assessment Plan (new programs have their initial review scheduled three years after launch)

These mechanisms, along with faculty and Curriculum Committee oversight, ensure continuous program improvement and objective measurement of learning outcomes.

4. Course Requirements and Descriptions

The Digital Forensics certificate consists of 12 graduate credits, delivered across four 3-credit courses: three required core courses and one elective. This structure mirrors the majority of SANS.edu's existing post-baccalaureate certificates, and supports timely program completion for working professionals.

SANS.edu Course	SANS Class	GIAC Exam	Credit Hours
ISE 6498	FOR498: Digital Acquisition and Rapid Triage	GBFA: GIAC Battlefield Forensics and Acquisition	3
ISE 6500	FOR500: Windows Forensic Analysis	GCFE: GIAC Certified Forensic Examiner	3
ISE 6585	FOR585: Smartphone Forensic Analysis In-Depth	GASF: GIAC Advanced Smartphone Forensics Certification	3
ISE XXXX	Elective (see elective course options below)	GIAC exam	3
		Total Required Credits	12

Core Course Descriptions

ISE 6498: Digital Acquisition and Rapid Triage

SANS Class: FOR498: Digital Acquisition and Rapid Triage

Assessment: GIAC Battlefield Forensics and Acquisition (GBFA)
Credit Hours: 3

This course provides the skills to identify the many and varied data storage mediums in use today, and how to collect and preserve this data in a forensically sound manner despite how and where it may be stored. The course covers digital acquisition from computers, portable devices, networks, and the cloud, and teaches rapid triage – the art and science of identifying and starting to extract actionable intelligence from a hard drive in 90 minutes or less.

This course prepares students to:

- Collect data from PCs, Macs, tablets, smartphones, RAM, virtual machines, and cloud environments
- Perform evidence acquisition while maintaining forensic soundness and chain of custody
- Execute rapid triage workflows to generate actionable intelligence in 90 minutes or less
- Capture volatile data and memory from live systems during active investigations
- Manage scenes efficiently to preserve and prioritize critical data
- Acquire evidence from enterprise environments including Exchange, SharePoint, and network repositories
- Utilize industry-standard open-source tools and SANS-provided environments for hands-on collection and analysis

ISE 6500: Windows Forensic Analysis

SANS Class: FOR500: Windows Forensic Analysis
Assessment: GIAC Certified Forensic Examiner (GCFE)
Credit Hours: 3

This course builds comprehensive forensics knowledge of Microsoft Windows (covering all Windows versions through Windows 11). It provides the means to recover, analyze, and authenticate forensic data, track user activity on the network, and organize findings for use in incident response, internal investigations, intellectual property theft inquiries, and civil or criminal litigation. Students can use this knowledge to validate security tools, enhance vulnerability assessments, identify insider threats, track hackers, and improve security policies. Detailed and real-world exercises teach the tools and techniques that every investigator should employ step-by-step to solve a forensic case. The course culminates in the GIAC Certified Forensic Examiner certification; one of the most respected credentials in the digital forensics community.

This course prepares students to:

- Conduct in-depth forensic analysis of Windows operating systems and media exploitation
- Identify artifact and evidence locations to answer crucial questions
- Become tool-agnostic by focusing your capabilities on analysis
- Extract critical findings and build an in-house forensic capability
- Establish structured analytical techniques to be successful in any security role

ISE 6585: Smartphone Forensic Analysis In-Depth

SANS Class: FOR585: Smartphone Forensic Analysis In-Depth
Assessment: GIAC Advanced Smartphone Forensics (GASF)
Credit Hours: 3

This mobile forensics course provides examiners and investigators with advanced skills to detect, decode, decrypt, and correctly interpret evidence recovered from mobile devices. FOR585 is continuously updated to keep up with the latest file formats, malware, smartphone operating systems, third-party applications, acquisition shortfalls, extraction techniques (how to get full file system or physical access) and encryption. It offers the most unique and current instruction to arm students with mobile device forensic knowledge they can immediately apply to cases they're working on the day they get back to work.

The course includes hands-on labs and a final forensic challenge to ensure that students not only learn the material, but can also execute techniques to manually recover data. Some labs allow users to "choose their own adventure" so that students who may need to focus on a specific device can select relevant labs and go back to the others as time permits.

This course prepares students to:

- Apply advanced smartphone forensic tools and techniques
- Understand smartphone file systems and data storage
- Identify data origins to prevent false evidence
- Recover hidden or obfuscated mobile data
- Investigate compromised smartphones and malware
- Overcome encryption and extract protected data
- Use advanced analysis methods in a simulated investigation

Elective Course Options (Choose One, 3 Credits)

Students select **one elective** from the approved list, which includes options from two related categories:

Digital Forensics Elective Options

- ISE 6518: Mac & iOS Forensic Analysis
  (FOR518 + GIME)

- ISE 6508: Advanced Incident Response, Threat Hunting & Digital Forensics
  (FOR508 + GCFA)

- ISE 6572: Advanced Network Forensics
  (FOR572 + GNFA)

- ISE 7610: Reverse-Engineering Malware
  (FOR610 + GREM)

- ISE 6497: Practical OSINT
  (SEC497 + GOSI)

- ISE 6587: Advanced OSINT Gathering & Analysis
  (SEC587 + GSOA)

Incident Response Elective Options

These remain DF-adjacent and valuable to forensics specialists, but are more IR-focused. Catalog language will clarify the distinction so students can make informed choices.

- ISE 7608: Enterprise-Class Incident Response & Threat Hunting
  (FOR608 + GEIR)

- ISE 6509: Enterprise Cloud Forensics & Incident Response
  (FOR509 + GCFR)

- ISE 6577: Linux Incident Response & Threat Hunting
  (FOR577 + GLIR)

- ISE 6578: Cyber Threat Intelligence
  (FOR578 + GCTI)

Electives enable specialization in complementary investigative competencies such as:

- threat intelligence
- cloud forensic analysis
- network artifact reconstruction
- forensic automation and scripting

- advanced threat hunting.

Elective course descriptions are included in the SANS.org academic catalog and follow the same structure and rigor as the core courses.

The program design satisfies all requirements of COMAR 13B.02.03.10. The curriculum is academically coherent, aligned to validated learning outcomes, and delivered by experienced forensic professionals. The integration of ANSI-accredited GIAC certification exams ensures that graduates demonstrate mastery of applied forensic skills at a level recognized across federal, military, and commercial investigative environments.

5. General Education Requirements

As a post-baccalaureate certificate program, the Digital Forensics program does not include general education requirements.

6. Specialized Accreditation or Graduate Certification Requirements

Each student who earns a SANS.edu Digital Forensics post-baccalaureate certificate will have achieved certification in four areas of cybersecurity using Global Information Assurance Certifications (GIAC).

7. Contract with Another Institution or Non-Collegiate Organization

Courses proposed for inclusion in this program are authored and taught by members of the faculty of the SANS Technology Institute. Commensurate with the approval of the SANS Technology Institute as a degree-granting institution in the State of Maryland in 2005, and as reviewed and accredited by the Middle States Commission on Higher Education, the SANS Technology Institute will continue to engage the support services of its parent, the Escal Institute for Advanced Technologies (d/b/a/ SANS Institute) and its sister subsidiary, GIAC. The agreements are not designed specifically for the Digital Forensics program, but as supporting structures for SANS.edu, these agreements support the delivery and management of this program. The MOUs have enabled all SANS.edu degree programs since the college was established, and were most recently reviewed and approved during the Middle States accreditation team visit.

Under a formal Memorandum of Understanding (MOU), SANS.edu outsources to SANS Institute (also known as SANS.org – SANS.edu'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, SANS.edu benefits from SANS.org's economies of scale, and transforms typically high-fixed-cost elements into manageable, smaller variable costs.

SANS.edu also benefits from its relationship with Global Information Assurance Certification (GIAC), a sister company also owned by SANS.org. 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 SANS.edu 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 GIAC 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 SANS.edu's Digital Forensics 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.

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

8. Enrolled Student Communications

SANS.edu 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 SANS.edu's existing graduate programs on the following web pages:

- Graduate admissions: https://www.sans.edu/admissions/graduate/
- Master's degree academic page: https://www.sans.edu/cyber-security-programs/masters-degree
- Graduate certificates academic page: https://www.sans.edu/graduate-certificates/

Once enrolled, new students attend orientation before registering for their first course. During orientation (outlined at https://www.sans.edu/students/orientation), students learn about modalities, faculty/student interaction, learning management systems, costs and

payment policies, and academic support services available. As a final stage of orientation, students meet with their individual advisor to discuss course and degree requirements and any questions that the students have a result of completing orientation.

9. Prospective Student Communications

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

H. Adequacy of Articulation

Articulation agreements are not expected to be applicable to this program.

The certificate:

- is post-baccalaureate
- requires a completed bachelor's degree
- does not accept lower-division coursework
- is not part of a transfer pathway.

This is compliant with COMAR 13B.02.03.19.

I. Adequacy of Faculty Resources

1. Program Faculty

The SANS.edu faculty is comprised of and appointed from individuals who have achieved the status of being "SANS Certified Instructors," an industry-recognized demarcation of technical achievement practiced in the field, superior teaching effectiveness and student engagement as exemplified in the classroom and online, and successful completion of a competitive development process that employs both student and peer-faculty feedback to prove that the instructors possess these qualities.

Among the faculty are people who are called upon to investigate attacks on the U.S. government and our largest commercial enterprises, who are entrusted to teach practitioners of cybersecurity at the highest and most sensitive (classified) levels, and who through their professional practice and research advance our understanding of cyber threats and potential remediation, and then transmit that knowledge forward to our students and the larger community.

Even beyond their superlative technical abilities, our faculty have skills as teachers that truly set them apart and allow them to impart sometimes dense technical lessons with enthusiasm, applicable real-world examples, and charismatic engagement. While a handful of faculty members serve in full-time teaching and research roles, most are scholar-practitioners who teach less than full-time for the school so that they can engage in the practice of cybersecurity, keep their skills advanced and current, and feed their experiences and learnings back into the courses and class discussions.

Faculty for this program includes the following individuals:

Faculty: Heather Barnhart

Appointment Type: Permanent
Status: Full-time
Terminal Degree Title and Field: B.S. Forensic and Investigative Science
Academic Rank/Title: Professor / SANS Fellow
Course(s) taught:
ISE 6500: Windows Forensic Analysis; ISE 6585: Smartphone Forensic Analysis In-Depth
Professional Certifications:
GIAC: GASF, GCFE
Other: CFCE, EnCE, CCO, CCPA

Heather Barnhart is the Dean of Faculty for the SANS Technology Institute, DFIR Curriculum Lead, Head of Faculty at the SANS Institute, and a SANS Faculty Fellow. She

brings nearly two decades of experience spanning high-profile law enforcement, government, and industry investigations, including analysis of Osama Bin Laden's digital media and evidence in the Idaho murders case. Heather leads and teaches SANS courses in Windows forensics and smartphone forensics and has authored DFIR course materials, publications, and widely used field resources. Her teaching emphasizes clarity, repeatable workflows, and operational readiness for real-world investigations.

Faculty: Tarot ("Taz") Wake

Appointment Type: Permanent
Status: Part-time (Adjunct)
Terminal Degree Title and Field: BSc (Hons) Open, Physics, Environment and Criminology
Academic Rank/Title: Assistant Professor / SANS Principal Instructor
Course(s) taught:
ISE 6577: Linux Incident Response & Threat Hunting; ISE 6508: Advanced Incident Response, Threat Hunting & Digital Forensics
Professional Certifications:
GIAC: GCFA, GCFE, GCIH, GCUX, GMON, GDAT, GXPN, GPYC
Other: CISSP, CPP, CRISC, CISM, CEH, C|CISO

Taz is the author of SANS ISE 6577 (Linux IR & Threat Hunting) and an instructor for ISE 6508 (Advanced IR & DFIR). His 20+ year career spans SIGINT, HUMINT, counterintelligence operations, enterprise CSIRT leadership, and IR program development for major global organizations. As Director at Halkyn Consulting, he builds SOCs and IR capabilities across industries. His teaching combines intelligence-driven analysis, offensive/defensive insight, and practical techniques for enterprise-scale investigations.

Faculty: Eric Zimmerman

Appointment Type: Permanent
Status: Part-time (Adjunct)
Terminal Degree Title and Field: B.S. Computer Science/Mathematics
Academic Rank/Title: Associate Professor / SANS Senior Instructor
Course(s) taught:
ISE 6498: Digital Acquisition and Rapid Triage
Professional Certifications:
GIAC: GCFE, GCFA
Other: Award-winning forensic tool developer; FBI U.S. Attorney's Award recipient

Eric Zimmerman is a former FBI Special Agent and Senior Director at Kroll specializing in large-scale digital forensics and investigative tooling. He is the creator of more than 50 forensic tools used by thousands of investigators worldwide and author of the *X-Ways*

Forensics Practitioner's Guide. As co-author of ISE 6498, he brings deep expertise in high-speed triage, low-level artifact interpretation, and forensic automation.

Faculty: Rob T. Lee

Appointment Type: Permanent
Status: Full-time
Terminal Degree Title and Field: MBA, International Business
Academic Rank/Title: Professor / SANS Fellow
Course(s) taught:
ISE 6500: Windows Forensic Analysis
Professional Certifications:
GIAC: GSE, GCFA, GCIH
Other: Creator of SIFT Workstation; major ICS/DFIR thought leader

Rob Lee is Chief AI Officer and Chief of Research at SANS Institute and one of the most influential figures in modern DFIR. A former Air Force cyber operations officer with NSA and CIA experience, Rob pioneered timeline analysis, created the SIFT workstation, and has led major global investigations, including CRASHOVERRIDE and the Ukraine power-grid attack analysis. His instruction blends technical depth with investigative leadership and operational clarity.

Faculty: Domenica (Lee) Crognale

Appointment Type: Permanent
Status: Part-time (Adjunct)
Terminal Degree Title and Field: M.S. in Cybersecurity Management
Academic Rank/Title: Lecturer / SANS Certified Instructor
Course(s) taught:
ISE 6585: Smartphone Forensic Analysis In-Depth
Professional Certifications:
GIAC: GASF
Other: EnCE, CCE, CISSP

Domenica Crognale is a digital forensics instructor, practitioner, and co-author of ISE 6585. She has spent 15 years supporting investigations within U.S. federal law enforcement and intelligence agencies and has trained military special forces, the Coast Guard, FBI, and others. Her expertise spans mobile application analysis, encrypted communications, and mobile IR workflows, with a teaching approach built on real investigative challenges.

Faculty: Full List

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

Table 0-1

Name	Degree	Field of Degree	Academic Title Rank	Status	Course(s)	Professional Certifications
Heather Barnhart	B.S.	Forensic and Investigative Science	Professor / SANS Fellow	Full-time	ISE 6500; ISE 6585	**GIAC:** GASF, GCFE **Other:** CFCE, EnCE, CCO, CCPA
Rob T. Lee	MBA	International Business	Professor / SANS Fellow	Full-time	ISE 6500	**GIAC:** GSE, GCFA, GCIH **Other:** SIFT creator; ICS/DFIR leader
Kevin Ripa	None	GIAC Certified + Extensive Field Experience	Lecturer / SANS Certified Instructor	Adjunct	ISE 6498	**GIAC:** GCFE, GCFA, GSEC **Other:** CCE, CEH (expired)
Eric Zimmerman	B.S.	Computer Science & Mathematics	Associate Professor / SANS Senior Instructor	Adjunct	ISE 6498	**GIAC:** GCFE, GCFA **Other:** FBI U.S. Attorney's Award; DFIR tool developer
Domenica (Lee) Crognale	M.S.	Cybersecurity Management	Lecturer / SANS Certified Instructor	Adjunct	ISE 6585	**GIAC:** GASF **Other:** EnCE, CCE, CISSP
Tarot ("Taz") Wake	BSc (Hons)	Physics, Environment & Criminology	Assistant Professor / SANS Principal Instructor	Adjunct	ISE 6508; ISE 6577	**GIAC:** GCFA, GCFE, GCIH, GCUX, GMON, GDAT, GXPN, GPYC **Other:** CISSP, CPP, CRISC, CISM, CEH, C
Sarah Edwards	M.S.	Information Assurance	Associate Professor / SANS Senior Instructor	Adjunct	ISE 6518	**GIAC:** GREM, GASF, GCFE **Other:** Mac/iOS forensics expertise
Phil Hagen	B.S.	Computer Science	Associate Professor / SANS Senior Instructor	Adjunct	ISE 6572	**GIAC:** GCFA, GNFA, GREM
Lenny Zeltser	MBA; B.S.E.	Business Administration; Computer Science	Professor / SANS Fellow	Adjunct	ISE 6610	**GIAC:** GSE, GREM **Other:** REMnux

						creator; malware research leader
Anuj Soni	M.S.	Information Systems Management, Information Security	Lecturer / SANS Certified Instructor	Adjunct	ISE 6610	**GIAC:** GREM **Other:** Malware IR specialist
Matt Edmondson	GIAC	GIAC Certified + Extensive Field Experience	Lecturer / SANS Certified Instructor	Adjunct	ISE 6497; ISE 6587	**GIAC:** GCFA, GREM, GPEN, GCIH, GWAPT, GMOB, GCFE, GCIA, GSEC, GOSI, GISF, GISP **Other:** OSCP
Marcus Guevara	M.S.	Cybersecurity	Lecturer / SANS Certified Instructor	Adjunct	ISE 6608	**GIAC:** (IR/DFIR GIAC set not enumerated) **Other:** OSCP; military cyber operations
Pierre Lidome	B.S.	Electrical Engineering	Lecturer / SANS Certified Instructor	Adjunct	ISE 6509	**GIAC:** GCTI, GCFA, GCFR **Other:** CCE, CISM
Megan Roddie-Fonseca	M.S.; M.S.	Digital Forensics; Information Security Engineering	Lecturer / SANS Certified Instructor	Adjunct	ISE 6509	**GIAC:** GSE, GX-IH, GX-IA, GCFR, GNFA, GCIA, GCTI, GSEC, GCFA, GCIH **Other:** MITRE ATT&CK credentials
Rebekah Brown	M.A.; B.A.	Homeland Security with Cybersecurity; International Relations	Lecturer / SANS Certified Instructor	Adjunct	ISE 6578	**GIAC:** GCTI **Other:** Cyber threat intelligence specialist
David Cowen	B.S.	Computer Science	Lecturer / SANS Certified Instructor	Adjunct	ISE 6509	**GIAC:** GCFE, GCFR **Other:** CISSP
Mathias Fuchs	M.S./M. Eng (equiv.)	Biomedizinische Informatik	Assistant Professor / SANS Principal Instructor	Adjunct	ISE 6508	**GIAC:** GCFA, GREM, GRID **Other:** CISA
Steve Anson	M.S.	Computer Science	Associate Professor / SANS Senior Instructor	Adjunct	ISE 6508	**GIAC:** GCFA, GCIH, GDAT, GPEN, GPYC **Other:** CISSP, EnCE, CCME

2. Faculty Recruitment and Development

One of the most serious responsibilities of the administration after student learning is the continued development and recruitment of qualified faculty. Especially since the institute

is committed to using only Scholar/Practitioners of a Master Teacher caliber, continuous development and recruitment is critical to the sustainability of the college. To this end, the SANS Technology Institute and the affiliated SANS Institute partner for faculty development. The high-level roadmap for faculty development is illustrated in Figure I-1.

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

Figure 0-1

Faculty Level Definitions

Mentor / TA

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

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

Community Instructor / TA

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

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

Trial Instructor / Supervised Instruction / TA

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

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

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

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

Certified Instructor

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

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

Senior Instructor

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

Faculty members who consistently achieve the highest evaluated ratings and who additionally have more than 240 course contact hours each year may qualify as Senior Instructors. Senior Instructors typically have additionally demonstrated significant leadership within the community of practice, perhaps through the development of course material used within the college or an affiliated entity.

Faculty Fellow

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

While a Faculty Fellow does not receive any additional privileges within the college, it is expected that those receiving the Faculty Fellow distinction maintain a leadership position

not only within his respective community of practice, but also among the faculty. These individuals should take a real interest in newly promoted faculty and strive to make them feel welcome in the faculty ranks. Faculty Fellows are also expected to be willing to come to the table when a mentor is needed for a fellow faculty member or potential faculty member who is struggling to meet or maintain his qualifications.

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

Faculty Development Opportunities

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

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

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

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

J. Adequacy of Library Resources

(Outlined in COMAR 13B.02.03.12)

The SANS Technology Institute maintains robust digital library holdings, research repositories, and technical resources that fully support the Post-Baccalaureate Certificate in Digital Forensics. These resources already underpin SANS.edu's existing master's degree and post-baccalaureate certificates and require no additional acquisitions for this program. The available library and research infrastructure exceeds what is necessary for a 12-credit graduate program in Digital Forensics. No additional library investments are required for program launch or sustainability.

SANS Information Security Reading Room

The SANS Reading Room contains more than 2,900 peer-reviewed research papers, authored by practitioners, researchers, and SANS.edu graduate students. These publications span:

- Windows forensic artifact analysis
- Cloud and SaaS forensics
- Mobile device forensic techniques
- Memory forensics
- Timeline reconstruction
- Investigative methodologies
- Incident response case studies

Digital Forensics certificate students would have unlimited access to this collection. The Reading Room is updated weekly, providing current and relevant investigative insights reflecting emerging threats, tools, and forensic methods.

EBSCO "Computers & Applied Sciences Complete" Database

SANS.edu provides students with unlimited access to EBSCO's full-text Computers & Applied Sciences Complete database, which includes:

- 650+ active journals and magazines
- 520+ active full-text peer-reviewed journals
- 320+ peer-reviewed journals with no embargo restrictions

Relevant titles cover:

- Digital forensics and evidence analysis
- Mobile and cloud forensics

- Information security and cybersecurity engineering
- Applied computing, operating systems, and network analysis

SANS.edu Cyber Research Repository

SANS.edu maintains an extensive archive of graduate-level research projects, theses, and capstone work produced by SANS.edu master's students. These papers offer applied, practitioner-oriented research on:

- forensic tool validation
- malware and memory forensics
- cloud logging and artifact correlation
- intrusion timeline construction
- forensic acquisition methodologies

Digital Forensics Laboratory Resources

Every student enrolled in FOR498, FOR500, and FOR585 receives access to comprehensive, professionally maintained virtual laboratory environments that include:

- forensic imaging utilities
- memory acquisition and analysis tools
- Windows artifact analysis suites
- mobile device extraction and analysis frameworks
- timeline and artifact correlation tools
- cloud forensic utilities
- Python-based forensic automation scripts

These lab environments are designed and maintained by SANS DFIR curriculum authors and serve as a core "learning resource" essential to modern forensic education.
No additional licenses, software, or hardware acquisitions are required to operate this program.

SANS Internet Storm Center (ISC) Handler Diaries and Archives

The SANS Internet Storm Center provides students with access to:

- global threat data feeds
- handler diaries analyzing emerging attack trends
- case studies highlighting forensic artifacts and intrusion patterns
- the DShield database for network and malware telemetry

These resources support student familiarity with real-world forensic indicators and investigative context. 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, these briefings 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.

SANS Security Policy Collection

SANS.edu provides access to 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. These can be used as references for:

- forensic reporting
- chain-of-custody workflows
- incident documentation
- organizational evidence-handling procedures

These materials help students situate technical work within organizational and legal frameworks.

Online Learning Management System (LMS) & Course Materials

The LMS serves as a central portal for:

- lecture notes and forensic workbook materials
- digital textbooks and reference guides
- supplemental reading packets
- lab instructions, toolkits, and datasets
- faculty Q&A archives
- asynchronous review materials

All course materials for the Digital Forensics certificate will be provided digitally and remain available throughout the program.

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

The SANS Newsletter Collection helps keep students up to date with the high-level perspective of the latest security news.

The Security Glossary

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 Intrusion Detection FAQs

Contains 118 authoritative discussions of the primary topics that arise when planning and implementing intrusion detection technologies. The collection is available at http://www.sans.org/security-resources/idfaq/.

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

(Outlined in COMAR 13B.02.03.13)

The SANS Technology Institute's existing physical, technical, and instructional infrastructure is fully adequate to support the Post-Baccalaureate Certificate in Digital Forensics. All required lab environments, online classrooms, virtual toolkits, technical services, administrative systems, and support structures are already in operation at scale.

No new facilities, equipment, or infrastructure investments are required for this program.

1. Physical Facilities, Infrastructure and Instruction Equipment

The SANS Technology Institute has all necessary physical facilities, technical infrastructure, and instructional equipment required to deliver the Post-Baccalaureate Certificate in Digital Forensics. Because SANS.edu is an established leader in distance-delivered cybersecurity education, no new facilities, technology investments, or instructional resources are required for the implementation or long-term operation of this program, which will use the same hybrid delivery model as existing certificate prorgams.

The Digital Forensics certificate will use the same fully developed, high-availability online ecosystems that support SANS.edu's existing post-baccalaureate certificates and master's degree programs, including the Software Supply Chain Security certificate, approved in 2023. SANS's online technology currently serves more than 18,000 students each year. This is not capacity-constrained, and is available globally and around-the-clock.

This program will be offered in combinations of various online modalities and residential institutes. More than 400 residential institutes are routinely available to students each year, with a cumulative capacity of more than 40,000 students.

Finally, building upon over a decade of experience in delivering synchronous and asynchronous online education, SANS has improved and expanded online delivery capabilities to include a "Live Online" format, which replicates a residential learning experience but offers full location flexibility for the learner. Thus, the proposed program will easily be accommodated in the existing in-person training programs.

2. Instructional Infrastructure and Technology

SANS.edu leverages the globally recognized SANS instructional platforms that support more than 40,000 cybersecurity learners annually. These platforms are already optimized for:

- graduate-level online instruction
- forensics-focused hands-on lab delivery
- real-time student engagement
- large-scale, high-bandwidth live events
- asynchronous self-paced learning

The following modalities will be available to students in this program:

Live Online (Synchronous)

A fully interactive online classroom environment featuring real-time instructor engagement, shared terminal sessions, breakout lab support and structured opportunities for Q&A. This is a real-time remote-learning modality that mirrors in-person SANS events, with dedicated staff facilitating remote learner participation and lab support.

OnDemand (Asynchronous)

A high-quality, self-paced modality offering pre-recorded instructor lectures, integrated lab demonstrations, in-platform quizzes and checkpoints, and access to virtual forensic tools and environments.

These modalities meet or exceed expectations for graduate-level instruction and fully satisfy COMAR requirements for distance education infrastructure.

L. Adequacy of Financial Resources (Tables 1 & 2)

Table 1: Program 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)	228,000	364,800	376,200	421,800	421,800
a. Number of F/T Students	20	32	33	37	37
b. Annual Tuition/Fee Rate	11,400	11,400	11,400	11,400	11,400
c. Total F/T Revenue (a x b)	228,000	364,800	376,200	421,800	421,800
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)	**228,000**	**364,800**	**376,200**	**421,800**	**421,800**

Table 2: Expenditures

Expenditure Categories	2025	2026	2027	2028	2029
1. Faculty (b + c below)	11,250	24,000	21,750	23,625	31,125
# FTE	N/A	N/A	N/A	N/A	N/A
Total Salary	6750	14,400	13,050	14,175	18,675
Total Benefits	4500	9600	8700	9450	12,450
2. Admin. Staff (b + c below)	352,800	386,400	428,400	470,400	512,400
# FTE	0.2	0.5	0.5	0.5	0.7
Total Salary	12,000	30,000	30,000	30,000	42,000
Total Benefits	4800	12,000	12,000	12,000	16,800
Support Staff (b + c below)	0	0	0	0	0

# FTE	0	0	0	0	0
Total Salary	0	0	0	0	0
Total Benefits	0	0	0	0	0
Technical Support and Equipment	0	0	0	0	0
Library	0	0	0	0	0
New or Renovated Space	0	0	0	0	0
Other Expenses	90,000	147,000	147,000	155,400	155,400
TOTAL (Add 1-7)	**118,050**	**213,000**	**210,750**	**221,025**	**245,325**

Finance Data: Narrative

The financial resources required to launch and sustain the Post-Baccalaureate Certificate in Digital Forensics are fully adequate. The certificate leverages SANS Technology Institute's existing academic infrastructure, faculty, administrative support systems, and contractual relationships with SANS and GIAC. As a result, no new facilities, faculty lines, or major operating expenses are required.

The program is designed as a scalable, tuition-supported certificate, consistent with SANS.edu's existing portfolio of post-baccalaureate online programs.

1. Narrative Rationale for Table 1: Program Resources

Reallocated Funds (Line 1)

No institutional funds will be reallocated from existing programs. The Digital Forensics certificate uses courses, faculty, online delivery technology, assessment systems, and operational services already in place. All required resources are fully absorbed by existing structures.

Tuition and Fee Revenue (Line 2)

The certificate follows SANS.edu's established tuition model:

$5,700 per 3-credit course, for a total program cost of $22,800 across four courses (12 credits).

Tuition includes:

- SANS course delivery
- textbooks and lab materials
- the corresponding GIAC certification exam, which serves as the academic assessment.

This bundled model is identical to tuition structures already approved by MHEC for otherSANS.edugraduate certificates, including the 2023 Software Supply Chain Security certificate.
Enrollment projections are intentionally conservative and reflect typical adoption patterns for new SANS.edu certificates.

These projections are consistent with historical SANS.edu certificate enrollments and reflect strong demand for Digital Forensics training across federal, state, and private-sector employers.

Because the program is delivered fully online or through existing instructional infrastructure, 100% of tuition revenue contributes to program stability and long-term viability.

Grants and Contracts (Line 3)

No external grants or contract funding are required for program implementation or sustainability. The program is not dependent on grant revenue and remains fully viable through tuition alone.

Other Sources (Line 4)

No other revenue sources are required.

2. Narrative Rationale for Table 2: Program Expenditures

Faculty (Line 1)

No new full-time faculty are required for this program. Faculty teaching the Digital Forensics certificate are already active instructors for:

- FOR498 (ISE 6498)
- FOR500 (ISE 6500)
- FOR585 (ISE 6585)
- approved elective courses

Because these courses run year-round through existing SANS in-person, Live Online, and OnDemand offerings, Digital Forensics certificate students represent a marginal increase in enrollment, not a new instructional burden.

Faculty costs are therefore recorded as a small proportional allocation ("marginal instructional cost") consistent with SANS.edu's financial modeling for other graduate certificates. Benefits follow the same proportional allocation.

Administrative Staff (Line 2)

Administrative staffing scales with enrollment. SANS.edu's current operational model supports approximately 150 certificate and master's students per full-time equivalent (FTE) staff member. Because certificate students require academic advising, GIAC exam coordination support, technical assistance for virtual labs, transcript and record management, the model assumes a gradual increase in administrative FTE to ensure adequate service quality.

This model is identical to the one MHEC approved in previous certificate proposals.

Support Staff (Line 3)

No support staff hires are required. Operational functions (LMS, IT support, financial services, registration, GIAC exam services) are provided through SANS.edu's existing service contracts with SANS and GIAC, as outlined in Appendix 1.

Equipment, Library, and Facilities (Lines 4–6)

No additional expenditures are required. All resources – lab environments, digital libraries, virtual machines, course materials, and technology platforms – already exist as part of SANS.edu's operating infrastructure.

Other Expenses (Line 7)

This category reflects variable per-student operational costs incurred under SANS.edu's Memoranda of Understanding with SANS and GIAC. These include:

- LMS licensing and maintenance
- virtual lab hosting
- event operations for Live Online courses
- exam processing fees beyond core GIAC exam costs
- student support and helpdesk services
- secure testing infrastructure
- general overhead related to course delivery

These costs scale predictably with enrollment and are consistent with SANS.edu's previously approved certificate programs.

M. Adequacy of Provisions for Evaluation of Program

Continuous, closed-loop evaluation has been the hallmark of SANS.edu programs since the school was established. SANS.edu 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."*

Level 1 – Daily Evaluation of Teaching Effectiveness

Every day, in every SANS.edu 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 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 the occasional case 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 learning modality. For On-Demand, the evaluation cycle is based on module completion rather than days, but the system is functionally equivalent.

Level 2 – Assessment via GIAC Examinations

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, many SANS.edu programs require a course in which students 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 GIAC Certified 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.

Level 3 – Evaluation of Program Outcomes

To evaluate program outcomes, SANS.edu 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, SANS.edu has implemented its formal Learning Outcomes Assessment Plan, as endorsed by the MSCHE evaluation team. Under this plan, each program undergoes a formal review by an evaluation team comprised of subject matter experts every five years.

This review process ensures alignment of (1) course outcomes to program learning objectives, of (2) program learning objectives to any capstone requirements, and of (3) both program learning objectives and capstone requirements to a survey of industry requirements.

This program proposal is based upon findings from a scheduled program review of a related Graduate Certificate program in 2025.

N. Consistency with Minority Student Achievement Goals

(Outlined in COMAR 13B.02.03.05)

The proposed Post-Baccalaureate Certificate in Digital Forensics supports the goals established under COMAR 13B.02.03.05 and the 2022 Maryland State Plan for Higher Education by expanding equitable educational access, promoting student success, and fostering innovation for historically underrepresented populations in cybersecurity. Maryland has one of the most diverse populations in the nation, yet minority students remain underrepresented in high-skill cybersecurity and digital forensics roles. This certificate directly supports Maryland's student achievement goals in four key ways:

1. Expanding Access Through Fully Online, Flexible Delivery

The certificate can be completed fully online through Live Online and OnDemand modalities. This format:

- eliminates geographic and transportation barriers;
- supports working adults balancing employment and family obligations;
- increases access for students unable to attend campus-based programs;
- enables participation from minority professionals across Maryland, including rural, suburban, and urban communities.

The fully online structure aligns with State Plan goals to increase equitable access to high-quality postsecondary learning.

2. Supporting Career Mobility and High-Demand Workforce Entry

Digital Forensics is a high-growth, high-wage field with significant shortages of practitioners across law enforcement, government, and industry. By creating a specialized forensic pathway, this certificate:

- enables minority professionals to enter or advance in DFIR careers;
- provides validated, employer-recognized credentials (GIAC certifications);
- increases opportunity for upward mobility into investigative, analytical, and leadership roles.

This supports the State Plan's "Success" goals for student progression, workforce placement, and reduced barriers to advancement.

3. Leveraging SANS CyberTalent Diversity Programs

SANS.edu collaborates closely with SANS CyberTalent, which operates multiple programs designed to support diverse learners, including:

- Fully funded Cyber Academies for various underserved populations
- Newcomer and reskilling pathways
- Maryland Cyber Workforce Academies, open to Maryland residents
- Scholarships and fully funded GIAC certification opportunities

These programs provide underrepresented students with no-cost access to foundational or advanced SANS courses, many of which can be applied as transfer credit toward SANS.edu certificates. Graduates of these academies – including those from minority-serving institutions – can apply their earned GIAC certifications toward the Digital Forensics certificate, reducing both time-to-completion and program cost.

4. Alignment with COMAR Requirements

Consistent with COMAR 13B.02.03.05, this program:

- expands opportunities for minority and educationally disadvantaged students
- improves pathways to high-demand cybersecurity careers
- contributes to Maryland's efforts to reduce equity gaps in STEM and cyber fields
- ensures underrepresented students have access to quality programs and flexible learning formats.

The Digital Forensics certificate strengthens Maryland's cyber workforce while supporting the State's commitment to equitable educational attainment. The certificate supports Maryland's minority achievement priorities by providing accessible online graduate education; engaging with SANS CyberTalent programs (including Diversity Academies); and offering stackable pathways for HBI graduates.

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

O. Relationship to Low Productivity Programs

The SANS Technology Institute does not operate any low-productivity programs as defined by the Maryland Higher Education Commission, and this proposed Post-Baccalaureate Certificate in Digital Forensics is not directly related to any program identified by the Commission as low-producing.

This certificate is a new, highly specialized program, which draws exclusively upon existing SANS courses, faculty, and infrastructure. It does not share curriculum, resources, or instructional capacity with any program that has been flagged for low productivity. It imposes no reallocation of faculty, administrative staff, budget, library resources, or facilities away from otherSANS.eduprograms.

Because the Digital Forensics certificate is a post-baccalaureate, revenue-supported, online-delivery program with clear workforce demand and a well-defined audience of working professionals, it is not expected to impact the productivity or viability of any existing degree or certificate offering.

Accordingly, no fiscal, academic, or operational adjustments to SANS.edu's current program portfolio are required for implementation of this certificate.

P. Adequacy of Distance Education Programs

The Post-Baccalaureate Certificate in Digital Forensics will be delivered through the SANS Technology Institute's established distance education modalities – Live Online and OnDemand – which have been repeatedly evaluated and approved as part of SANS.edu's existing MHEC-authorized programs. SANS.edu affirms that the program fully complies with the C-RAC Principles of Good Practice and the requirements of COMAR 13B.02.03.22.

1. Eligibility to Provide Distance Education

SANS.edu was approved by Middle States to deliver more than 50 percent of credit via distance modalities, following submission of a Substantive Change Request in 2014, so has now been offering high-quality online cybersecurity programs for more than a decade.

Distance learning is integral to the Institute's mission, strategic plan, and long-term academic model. The institution maintains robust infrastructure, governance, policies, and assessment processes that ensure ongoing quality and improvement across all online programs.

2. Compliance with C-RAC Guidelines

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

The two distance learning modalities available to students to complete the SANS technical course component are OnDemand and Live Online. Students who use the OnDemand platform are given access to a learning management system with modules pre-loaded into the system, and are also provided with printed course books containing written lectures and labs. Each module is a recording from an in-person course session. The learning management system allows students to revisit lectures and also complete quizzes to verify understanding. A recommended viewing schedule is included in course syllabi. Each SANS.edu course has a responsible faculty member, who is commonly the person that recorded the OnDemand course content. Teaching assistants, referred to as Subject Matter Experts (SMEs), are available for all OnDemand courses to help answer student questions or assist with lab issues.

The Live Online delivery modality allows students to participate in a course 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 SANS.edu course reviews student performance on exams and papers and assigns a grade at the end of the course.

1. Curriculum and instruction

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

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

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

If a student chooses a distance learning modality, that experience is comprised of the very same coherent, cohesive, and academically rigorous curriculum used for the course when taken via our traditional residential institute-based, in-person instructional format. The faculty member who oversees the SANS.edu 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 SANS.edu'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 SANS.edu was approved by Middle States to deliver more than 50 percent of 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 SANS.edu's OnDemand modalities, and once again found the measured learning outcomes to be the same among both groups (Table P-1).

Table 0-1: Comparison of GIAC Exam Score Performance via Live and OnDemand Modalities, 2014-2017

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

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

The learning outcomes of the courses included in the proposed program have been validated by the faculty as appropriately rigorous and broad, and are integrated into each course and measured quantitatively through standardized certification exams.

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

Teaching assistants, referred to as Subject Matter Experts (SMEs), are available for all OnDemand courses to help answer student questions or assist with lab issues.
The Live Online delivery modality allows students to participate in a course being offered through the in-person modality, but from their location of choice, enabled through a digital learning management system. Students meet during the same time that the in-person course meets. They can participate in classroom lectures by seeing and hearing the instructor, in addition to asking questions and participating in classroom discussion.

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

SANS.edu faculty members design all distance learning programs.

2. Role and mission

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

The distance education program at SANS.edu 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 SANS.edu's mission to develop leaders to strengthen enterprise and global information security.

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

The appropriateness of the technology SANS.edu uses for distance education has evolved over more than 15 years to be optimized for meeting the active learning needs of full-time working professionals, and it been assessed and approved by SANS.edu faculty. But that is not the end of the development process. The distance learning technology is continuously

evaluated through surveys completed by every one of the more than 3,000 cybersecurity professionals using it each day. If a course is not helping students master the key learning objectives, we hear about it quickly and fix the problems.

3. Faculty support

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

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

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

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

Instructor Guidelines for SANS Live Online Classes

What to Expect

During a SANS Live Online you will be teaching live students in the same room AND students at remote locations. To accomplish this, your on-site moderator will log into Zoom and our system will capture everything that is projected in the classroom. You will also wear a wireless microphone to transmit your voice to remote students. The moderator will also set up a webcam and broadcast video from the classroom.

All-day classes will be broken into two sessions: morning and afternoon. When you break for lunch please remind all students to log out of Zoom and to log into the afternoon session when they return. You will also need to do the same thing, so please return from your lunch break a few minutes early. The key to teaching a successful Live Online class is to always remember that you are teaching remote students; keep them engaged by promptly responding to their questions and periodically addressing them directly.

Advance Planning

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

Audio Tips

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

Starting Class

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

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

Teaching Tips

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

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

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

4. Students and Student Services

(a) 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 helpsSANS.edustudents 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.

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

seen at the Internet Storm Center, new technologies that are emerging, and analysis of security trends.

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

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

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

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

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

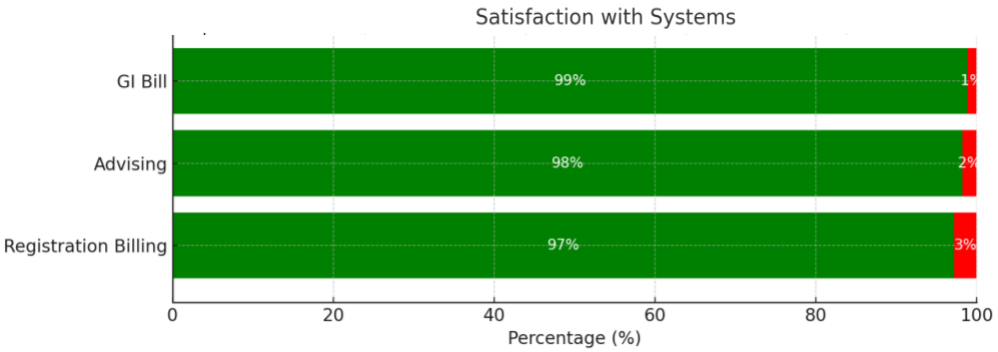

Figure P-1: Student Satisfaction with Student Management as Reported in the 2024 Student Experience Survey

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

Students in this program are required to have a Bachelor's degree and some industry experience. Those admitted will be sufficiently well versed in information technology to have scored sufficiently high on the cyber aptitude test and simulator to gain acceptance. Thus, they have the needed background, knowledge, and technical skills to use the distance learning modalities.

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

Advertising, recruiting, and admissions materials for the proposed Digital Forensics program are currently being drafted. SANS.edu has a solid record of meeting Middle States' high standards for transparency and accuracy in all its marketing and admissions materials and will continue to do so. Advertising, recruiting, and admissions materials for Graduate Certificate programs were available in the Resource Room during the 2017 MSCHE and MHEC evaluation team visit.

5. Commitment to support

(a) 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 SANS.edu.

(b) 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.

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

6. Evaluation and assessment

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

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

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

SANS.edu's online teaching practices are currently in use by more than 3,000 students, with over 50,000 students using the systems during the past ten years. Each of those students evaluates the effectiveness of the learning modality in every course, and SANS.edu continually improves practices to ensure those ratings continue to match or exceed live classroom training scores.

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

Ultimate student achievement in the proposed program will be measured by grades on the internationally standardized GIAC exams for each course in the program. SANS compares these scores in distance and in-person learning modalities. As shown in Table P-2, the GIAC test scores in distance learning are essentially identical to scores of students who used live, in-person residential training programs:

Table P-2: Comparison of GIAC Exam Score Performance via Live and OnDemand Modalities, 2014–2017

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

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

Appendix I. Contracts with Related Entities

The SANS Technology Institute (SANS.edu) 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 SANS.edu:

- **SANS.edu as an independent subsidiary** – SANS.edu 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 SANS.edu 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 SANS.edu's students to access world-class faculty and educational content from an otherwise small institution.

- **SANS.edu's faculty come from SANS** – SANS.edu's faculty is comprised of and appointed from the 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.

- **SANS.edu's programs designed by SANS.edu faculty** – SANS.edu'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, SANS.edu 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 SANS.edu 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 SANS.edu faculty member into the online version of the course, complete with the same labs and access to subject-matter experts online. SANS.edu 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** – SANS.edu'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 SANS.edu's programs are themselves ANSI-certified for quality and robustness. The use of those exams enables SANS.edu'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.

    - **SANS.edu-Specific Educational Elements and Courses** – SANS.edu's faculty creates many additional elements to augment the programs with written security memos and research, oral presentations, group projects, and other experiences designed to require high-level integrations of learning.

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

Memorandum of Understanding

between

The SANS Technology Institute ("STI")

and

The Escal Institute of Advanced Technologies ("SANS")

Agreement Published Date: June 1st, 2023

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

Purpose

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

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

Vision

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

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

Mission

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

Scope

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

Hours of Operations

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

Service Expectations

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

Accounting and Finance

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

Bursar & Registration

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

Human Resources

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

Marketing

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

Information Technology

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

Technical Course Maintenance & Presentation

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

Educational Residency

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

Service Constraints

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

- **Conformance Requirements** - Finance policy changes and Internal Revenue regulations may alter procedures and service delivery timeframes.
- **Dependencies** - Achievement of the service level commitment is dependent upon student and employee compliance with the policies and procedures of the STI enterprise.

Terms of Agreement

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

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

Periodic Quality Reviews

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

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

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

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

Service Level Maintenance

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

Issue Resolution

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

Payment Terms and Conditions

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

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

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

Appendix A:

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

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