SANS Technology Institute

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

ALAN PALLER
President

DAVID HOELZER
Dean of Faculty

JOHANNES ULLRICH, Ph.D.
Dean of Research

TIM CONWAY
ICSS Program Director

ERIC PATTERSON
Executive Director

SHELLEY MOORE
Assistant Director

BETSY MARCHANT
Assistant Director,
School Operations

July 31, 2018

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

Dear Dr. Fielder,

The SANS Technology Institute is pleased to submit the attached proposal to create a new Industrial Control Systems Security graduate certificate program. As the first program of its kind, in Maryland or anywhere, the STI ICSS graduate certificate will address the critical developing need of protecting our nation's essential infrastructure and will further establish Maryland as a leader in the field of cyber and information security.

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

Sincerely,

Alan Paller
President
SANS Technology Institute

PROPOSAL FOR A GRADUATE CERTIFICATE IN INDUSTRIAL CONTROL SYSTEMS SECURITY

SANS Technology Institute

MARYLAND HIGHER EDUCATION COMMMISSION

ACADEMIC PROGRAM PROPOSAL

PROPOSAL FOR:

__x__NEW INSTRUCTIONAL PROGRAM

____ SUBSTANTIAL EXPANSION/MAJOR MODIFICATION

____ COOPERATIVE DEGREE PROGRAM

__x__WITHIN EXISTING RESOURCES or__REQUIRING NEW RESOURCES

The SANS Technology Institute
Institution Submitting Proposal

October 1, 2018
Projected Implementation Date

Graduate Certificate
Award to be Offered

Industrial Control Systems Security
Title of Proposed Program

5199
Suggested HEGIS Code

11.1003
Suggested CIP Code

SANS Technology Institute
Department of Proposed Program

Tim Conway
Name of Department Head

Tim Conway
Contact Name

tconway@sans.org
Contact E-mail Address

(708) 738-9572
Contact Phone Number

President/Chief Executive Approval
Signature and Date

Monday, 30 July, 2018
Date Endorsed/Approved by Governing Board

Table of Contents

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

1. Program Description

The SANS Technology Institute (STI) proposes to launch a new program leading to a Graduate Certificate in Industrial Control Systems Security (ICSS). The proposed SANS Technology Institute graduate certificate program in ICSS is a 12-credit hour program with a cohesive set of learning outcomes focused on teaching applied technologies used to defend and secure industrial control systems, operations technology, or cyber-physical systems. The Industrials Control Systems Security graduate certificate program provides a broad and integrated mechanism for students to learn the essential security awareness, work-specific knowledge, and hands-on technical skills needed to secure automation and control system technology.

These systems often form the backbone of infrastructures identified as critical to national security, economic security, public health, or safety. Traditional defenses found in business or corporate IT environments are not always effective when applied to the industrial or operation technology space. Legacy equipment, proprietary hardware and software, non-traditional protocols, and consideration for the health and safety of equipment, personnel, and communities all add to the challenges of securing these environments. This proposed program will deliver a tailored solution to an emerging, critical, and widely unrecognized need.

ICSS graduate certificate students will complete three required courses and one elective course, earning at least three, and possibly four, industry-recognized certifications:

Required core courses (9 credit hours):

Students will take these three core courses:
ISE 6515 (SANS Course ICS410): ICS/SCADA Security Essentials | GICSP: Global Industrial Cyber Security Professional (3 credits)
ISE 6520 (SANS Course ICS515): ICS Active Defense and Incident Response | GRID: GIAC Response and Industrial Defense (3 credits)
ISE 6525 (SANS Course ICS 456): Essentials for NERC Critical Infrastructure Protection | GCIP: GIAC Critical Infrastructure Protection (3 credits)

Elective Course (3 credit hours)

Any 3-credit STI course with associated GIAC Certification, from the STI Course Catalog (3 credit hours)
RES 5500 Graduate Research Practicum with one of two required content experiences: (1) Hosted: Assessing and Exploiting Control Systems (2) Hosted: Critical Infrastructure and Control System Cybersecurity (3 credit hours)

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

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

2. Relation to STI Mission and Strategic Goals

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

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

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

1. Critical Need for the ICSS Program

The proposed ICSS graduate certificate program aligns directly with Maryland Core Goal #6: Cybersecurity and Critical Infrastructure Protection.[1] This goal states that,

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

[1] http://gohs.maryland.gov/va/ and http://www.mcac.maryland.gov/how_to_help/H2H_CIP/index.html

government services. Maryland should have a complete and prioritized inventory of critical infrastructure, including assets controlled by the private sector, and a system for securing high-priority targets or populations of interest.

Consisting of four sub-goals, each with a specific focus, Maryland's critical infrastructure program has been expanded and integrated into the State's intelligence fusion center to improve information sharing between law enforcement and the private sector.[2]

Whether publicly or privately held, industrial, manufacturing, transportation, and water and energy delivery systems are now nearly entirely controlled, automated, or monitored by computer networks, with parts of those systems necessarily connected in some fashion to the internet. Given this increasing connectivity, even unintentional and non-malicious events now have the potential to cascade quickly to affect large parts of a city or region. For example, the infamous 2003 Northeast blackout was triggered by a simple fault—a tree caused a transmission line short circuit—but within hours it became the largest blackout in U.S. history, owing to two computer/software errors that caused a lack of situational awareness from grid operators. A smaller but similar cascading failure occurred in 2011 in the southwestern United States, when a problem at a single substation in Arizona grew into a major outage across Southern California in a few minutes.

More ominously, with the continued emergence and technological evolution of asymmetric actors who have no interest in the status quo of society-at-large and who view the internet as not just a vehicle to generate revenue, to recruit, or to spread ideology but, instead, as a weapon system in an increasingly connected world, the development of highly skilled leaders leading the defense of industrial control systems is an essential step.

Cyber threat actors continue to demonstrate an increasing capability and intent to target industrial control systems. Since 2011, known or suspected hackers in several countries have run supervisory control and data acquisition (SCADA) exploitation attempts against US critical infrastructure. In September 2015, in testimony before the House Permanent Select Committee on Intelligence, former Director of National Intelligence James Clapper revealed that unknown Russian cyber actors had compromised the supply chains of at least three industrial control system vendors. He warned, "Politically motivated cyber-attacks are now a growing reality, and foreign actors are reconnoitering and developing access to U.S. critical infrastructure systems."

In subsequent hearings before the House Armed Services Subcommittee on Emerging Threats and Capabilities in March 2016, Admiral Mike Rogers, former commander of US Cyber Command and director of the National Security Agency (NSA), testified that "industrial control systems and SCADA probably is the next big area." In a separate forum, Rogers also noted that, with regards to a damaging attack upon the critical infrastructure of our nation, "It's not a matter of 'if,' it's a matter of 'when.' "[3]

[2] http://gohs.maryland.gov/va_accomplishments/

[3] http://www.businessinsider.com/nsa-chief-describes-3-biggest-cyber-threats-2015-10

Michael Assante, who served as the first Chief Security Officer of the North American Electric Reliability Corporation (NERC) and who is currently the Director of Industrials & Infrastructure at SANS, had this to say during his testimony to the Federal Energy Regulatory Commission on June 22, 2017, on the specific topic of providing a properly trained, educated, and led critical infrastructure workforce:

"The continued advancement of adversary techniques and capabilities requires constant vigilance, the formulation of flexible responses, and the need to build upon the protection that the standards afford to develop a workforce capable of defending power systems. Continued efforts from NERC focused on…specific technical, hands-on, cyber security training will continue to improve our overall capabilities and preparedness. This is an encouraging area where NERC Registered Entities are moving beyond the standards requiring awareness training towards specialized cybersecurity training for security and ICS staff."[4]

A report released in May 2018 by the Departments of Energy and Homeland Security noted a "number of 'gaps' preventing private electric utilities, government entities and other stakeholders from bolstering their ability to provide effective incident response in the event of a major cyber assault on the grid. These include a lack of clarity around the roles of specific organizations in responding to prospective cyber incidents; shortfalls in the electric sector's cyber workforce; a lack of effort to address supply chain vulnerabilities specific to the electric sector; and lackluster information sharing between private industry and the federal government."[5] Clearly, this set of complex and interwoven challenges will not be solved without effective leadership, public and private, which both understands the technical details of the electrical grid and the threats to it as well as how to successfully communicate with and persuade non-technical leaders to invest in the full range of necessary solutions.

Currently, we are unaware of any educational program which is specifically seeking to produce technically educated leaders who are prepared to design, champion, and manage the implementation and ongoing operation of state-of-the-art defenses in support of the full range of our society's critical infrastructure. In order to contribute to further synergy and partnership across the public-private divide being bridged by the State's fusion center, educated leaders in the private sector with expertise in industrial control systems will serve as force multipliers for Maryland's Core Goal #6. The STI ICSS graduate certificate program is intended to produce these leaders. With its strategic placement on the Eastern seaboard, in close proximity to the nation's capital and to other major metropolitan areas, and given its central placement in various transportation and energy networks, Maryland is an ideal home to this first-in-class program.

[4] https://www.ferc.gov/CalendarFiles/20170717080648-Assante,%20SANS%20Institute.pdf
[5] http://thehill.com/policy/cybersecurity/390065-federal-assessment-finds-gaps-in-preparation-for-electric-grid-attacks

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

Increase student success with less debt

The ICSS program will address the State Plan's goals to increase student success with less debt. Approximately 45% of our students fully fund their studies by way of employer tuition reimbursement. We have every reason to expect that manufacturing and utility employers will continue to increasingly invest in the leadership of their cyber security workforce in the same manner, especially given the significant number of our current graduate certificate students in other, currently existing programs who are employed in the manufacturing, transportation, or utilities sectors.

The ICSS program also targets elements of two other Strategies in the Maryland State Plan. Strategy 7 calls for special efforts to support veterans. Approximately 40% of our current study body is comprised of veterans, with nearly all of them using some combination of GI Bill benefits and employer tuition reimbursement to increase their knowledge and skills as they enter or further establish themselves in the civilian workforce. Increasingly, we are seeing recently separated veterans who have completed the SANS VetSuccess Immersion Academy[6] seeking to further their advancement in the field of information security by enrolling in an STI graduate program.

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

1. Market Demand

With its strong and growing number of manufacturing, transportation, and energy entities, Maryland is both a growth hub and a potentially vulnerable series of interconnected networks. Maryland currently boasts more than 3,700 manufacturing companies. Of these, 60 percent are categorized as "advanced," thus involving a highly efficient and automated production, logistics, or distribution network. Similarly, Maryland's central East Coast location provides connectivity to the largest power pool in North America. The PJM Interconnection (aka The Grid) is a regional system that shares power generation and distribution resources across all or parts of 13 states and the District of Columbia. Altogether, Maryland's 1,260 energy firms already generate some $8 billion in gross state product.

The ARC Advisory Group recently analyzed a UI LABS and ManpowerGroup workforce analysis which identified 165 data-centric jobs that will define the future of manufacturing in the United States. According to that report, "Jobs such as collaborative robotics specialist, **manufacturing cybersecurity strategist** and enterprise digital ethicist provide a window into the advanced skills and knowledge needed to put new technology into practice and remain globally competitive."[7] A factory adapting to the current tide of digitization will greatly depend on this modified, highly skilled workforce. Digitization is transforming the job market, creating a need for people with

[6] https://www.sans.org/cybertalent/cybersecurity-career/vetsuccess-academy

[7] https://www.arcweb.com/blog/reskilling-todays-industrial-workforce-ot-it-convergence-0

more advanced skills in manufacturing, to include those with the knowledge to understand and protect the digital networks behind the entire automation process.

A recent Forbes article discussed how ISACA, a leading a non-profit information security advocacy group, assessed the future trends in the information security workforce. According to ISACA, "If you're interested in a cyber security career, where should you look? Large health care, financial and global manufacturing firms need armies of cyber security professionals."[8]

Finally, Cyberseek, a workforce assessment project supported by the National Initiative for Cybersecurity Education (NICE) under the auspices of NIST, released a study on security career opportunities. In that study, they determine that job requirements as supplied by organizations seeking security talent indicate that post-graduate programs are valued, as well as specialized certifications.[9] The proposed STI ICSS program is designed to supply both of those credentials.

2. Current and Projected Supply of Prospective Graduates

Cybersecurity jobs are already an important part of Maryland's economy, comprising the second highest concentration of professional and technical workers among all fifty states. With the increasing recognition of the vulnerability of critical infrastructure and the need to better protect it, it is reasonable to expect that, in conjunction with the State Plan, (a) current members of Maryland's information security workforce will seek to transition to the specific protection of control systems, and (b) Maryland will continue to attract additional information security workers and separating military veterans who wish to enter into this challenging field.

With specific regards to the subset of information security employees within the industrial and infrastructure sector, a 2016 InTech/Automation survey indicates that 31% of respondents were 30+ year veterans. In their 2017 survey, that percentage dropped to 18.8%. Nationwide, this rapidly retiring workforce not being adequately replaced with younger workers. With more complex ICS systems, and with shorter system life-cycles, the capabilities of workers to be agile and to possess an expand skillset is increasing in order to stay relevant to the field. This likely requires greater workforce investments to build KSAs in their personnel, especially given the dynamic nature of industry threats to ICS systems that historically few experienced workers leaving the workforce have had to cope with legacy system.[10] Taken together, these factors represent a nascent opportunity for Maryland to train and provide specialized leaders for the protection of critical infrastructure.

[8] https://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/#685e23e75163

[9] http://cyberseek.org/pathway.html

[10] https://www.automation.com/salary-survey-results-2017

D. Reasonableness of Program Duplication

1. Similarities and Differences between the ICS Program and Other Programs Awarding the Same Degree

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

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

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

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

Degree to Be Awarded

Graduate certificate.

Specific Academic Content of the Program; Evidence of Equivalent Competencies

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

Alternative Means of Educational Delivery, including Distance Education

STI's ICSS program has the unique ability to offer students the flexibility to take their courses either through live in-classroom instruction or via our award-winning OnDemand distance-learning system. The STI ICSS program also enables students to enroll with an individualized, flexible academic plan that allows each of them, as per our admissions requirements, and to continue to work a full-time job while they complete the program.

Role and Mission

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

Admissions Requirements

STI's admission requirements for ICSS will be as already established for our existing graduate certificate programs:

- Have at least 12 months of professional work experience in information technology, security or audit

- Be employed or have current access to an organizational environment that allows you to apply the concepts and hands-on technical skills learned in the program

- Have earned a baccalaureate degree from a recognized college or university, or equivalent international education, with a minimum cumulative grade point average of 2.80

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

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

No HBI offers a comparable credential.

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

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

Generally, the ICSS program has no impact on the uniqueness or identity of any of the HBIs.

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

1. Program Outline and Requirements

Required Courses

Students will take these three core courses:
ISE 6515 (SANS Course ICS410): ICS/SCADA Security Essentials | GICSP: Global Industrial Cyber Security Professional (3 credits)
ISE 6520 (SANS Course ICS515): ICS Active Defense and Incident Response | GRID: GIAC Response and Industrial Defense (3 credits)
ISE 6525 (SANS Course ICS 456): Essentials for NERC Critical Infrastructure Protection | GCIP: GIAC Critical Infrastructure Protection (3 credits)

ISE 6515 ICS/SCADA Security Essentials (3 credits)

SANS class: ICS 410 ICS/SCADA Security Essentials
Assessment: GIAC GICSP
3 Credit Hours

ISE 6515 ICS/SCADA Security Essentials is an introductory study of how information technologies and operational technologies have converged in today's industrial control system environments. This convergence has led to a greater need than ever for a common understanding between the various groups who support or rely on these systems. Students in ISE 6515 will learn the language, the underlying theory, and the basic tools for industrial control system security in settings across a wide range of industry sectors and applications.

This course provides students with the essentials for conducting cybersecurity work in industrial control system environments. After spending years working with industry, we believe there is a gap in the skill sets of industrial control system personnel, whether it be cybersecurity skills for engineers or engineering principles for cybersecurity experts. In addition, both information technology and operational technology roles have converged in today's industrial control system environments, so there is a greater need than ever for a common understanding between the various groups who support or rely on these systems. Students in ICS410 will learn the language, the underlying theory, and the basic tools for industrial control system security in settings across a wide range of industry sectors and applications.

ISE 6520 ICS Active Defense and Incident Response (3 credits)

SANS class: ICS 515 ICS Active Defense and Incident Response
Assessment: GIAC GRID
3 Credit Hours

ISE 6520 will empower students to understand their networked industrial control system environment, monitor it for threats, perform incident response against identified threats, and learn from interactions with the adversary to enhance network security.

This class was developed from my experiences in the U.S. intelligence community and within the control system community dealing with advanced adversaries targeting industrial control systems.

ISE 6525 Essentials for NERC Critical Infrastructure Protection (3 credits)

SANS class: ICS 456 Essentials for NERC Critical Infrastructure Protection
Assessment: GIAC GCIP
3 Credit Hours

ISE 6525 empowers students with knowledge of the "what" and the "how" of the version 5/6 standards. The course addresses the role of FERC, NERC and the Regional Entities, provides multiple approaches for identifying and categorizing BES Cyber Systems and helps asset owners determine the requirements applicable to specific implementations. Additionally, the course covers implementation strategies for the version 5/6 requirements with a balanced practitioner approach to both cybersecurity benefits, as well as regulatory compliance.

The NERC Critical Infrastructure Protection Essentials course was developed by SANS ICS team members with extensive electric industry experience including former Registered Entity Primary Contacts, a former NERC officer, and a Co-Chair of the NERC CIP Interpretation Drafting Team. Together the authors bring real-world, practitioner experience gained from developing and maintaining NERC CIP and NERC 693 compliance programs and actively participating in the standards development process.

ISE 6715 Essentials for NERC Critical Infrastructure Protection (3 credits)

SANS class: AUD 507 Auditing Networks, Perimeters, and Systems
Assessment: GIAC GSNA
3 Credit Hours

ISE 6715 is organized specifically to provide a risk driven method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high level audit issues and general audit best practice, students have the opportunity to dive deep into the technical how to for determining the key controls that can be used to provide a level of assurance to an organization. Tips on how to repeatably verify these controls and techniques for continuous monitoring and automatic compliance validation are given from real world examples.

Electives Courses: (3 credit hours)

Any 3-credit STI course with associated GIAC Certification, from the STI Course Catalog (3 credit hours)
RES 5500 Graduate Research Practicum with one of two required content experiences: (1) Hosted: Assessing and Exploiting Control Systems (2) Hosted: Critical Infrastructure and Control System Cybersecurity (3 credit hours)

2. Educational Objectives and Intended Student Learning Outcomes

The five primary educational objectives of the program are to:

a) PLO1: Learn, integrate, practice, and demonstrate mastery of the essential knowledge, technical skills, and leadership abilities relevant to securing automation and control system technology.
b) PLO2: Utilize a broad range of current tools and technologies in the design and implementation of security solutions deployed across critical infrastructure organizations.
c) PLO3: Identify the information assets within an automation or control systems environment, classify them by value, and determine what management and technical controls can be used to monitor and audit them effectively and securely.
d) PLO4: Develop a program for analyzing the risk to the information assets in an automation or control systems environment and determine which technical and management controls can mitigate, remove, or transfer that risk.
e) PLO5: Articulate important attacker techniques, analyze the traffic that flows on automation or control system networks, and identify indications of an attack, engage in testing and audit within their organization, and respond to incidents associated with these activities within their organization

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

ISE 6515 (SANS Course ICS410): ICS/SCADA Security Essentials:

- Students will develop and reinforce a common language and understanding of Industrial Control System (ICS) cybersecurity as well as the important considerations that come with cyber-to-physical operations within these environments. Each student will receive a programmable logic controller (PLC) device to keep. The PLC contains physical inputs and outputs that will be programmed in class and mapped to an operator interface, or HMI, also created in class. This improved hardware-enabled approach provides the necessary cyber-to-physical knowledge that allows students to better understand important ICS operational drivers and constraints that require specific safety protection, communications needs, system management approaches, and cybersecurity implementations. Essential terms, architectures, methodologies, and devices are all covered to build a common language for students from a variety of different roles.

- Students will develop a better understanding of where specific attack vectors exist and how to block them, starting at the lowest levels of the control network. Students will look at different technologies and communications used in Perdue Levels 0 and 1, the levels that are the most different from an IT network. Students will capture fieldbus traffic from PLCs look at what other fieldbus protocols used in the industry. Students will analyze network captures containing other control protocols that traverse Ethernet-only networks and TCP/IP networks, set up a simulated controller, and interact with it through a control protocol.

- Students will learn about different methods to segment and control the flow of traffic through the control network. Students will explore cryptographic concepts and how they can be applied to communications protocols and on devices that store sensitive data. Students will learn about the risks of using wireless communications in control networks, which wireless technologies are commonly used, and available defenses for each. After a hand-on network forensics exercise where students follow an attacker from phishing campaign to HMI breach, students will look at HMI, historian, and user interface technologies used in the middle to upper levels of the control network, namely Perdue Levels 2 and 3, while performing attacks on HMI web technologies and interfaces susceptible to password brute force attacks.

- Students will learn essential ICS-related server and workstation operating system capabilities, implementation approaches, and system management practices. Students will receive and work with both Windows- and Linux-based virtual machines in order to understand how to monitor and harden these hosts from attack. Students will examine concepts that benefit ICS systems such as system hardening, log management, monitoring, alerting, and audit approaches, then look at some of the more common applications and databases used in ICS environments across multiple industries. Students will explore attacks and defenses on remote access for control systems.

- Students will learn about the various models, methodologies, and industry-specific regulations that are used to govern what must be done to protect critical ICS systems. Key business processes that consider risk assessments, disaster recovery, business impact analysis, and contingency planning will be examined from the perspective of ICS environments. Students will work together on an incident response exercise that places them squarely in an ICS environment that is under attack. This exercise ties together key aspects of what has been learned throughout the course and presents students with a scenario to review with their peers. Specific incident-response roles and responsibilities are considered, and actions available to defenders throughout the incident response cycle are explored.

ISE 6520 (SANS Course ICS515): ICS Active Defense and Incident Response | GRID: GIAC Response and Industrial Defense:

- Students will learn how threat intelligence is generated, how to critically analyze reports, and the basic tenets of active defense functions. Students will become better analysts and critical thinkers by learning skills useful in day-to-day operations, regardless of their jobs and roles. Students will build a Programmable Logic Controller (PLC), will identify information available about assets online through Shodan, will complete an analysis of competing hypotheses, and will understand how to review threat intelligence reports.

- Students will use tools such as Wireshark, TCPdump, SGUIL, ELSA, CyberLens, Bro, NetworkMiner, and Snort to map an ICS network, collect data, detect threats, and analyze threats to drive incident response procedures. Students will be introduced to a lab network and an advanced persistent threat (APT) that is present on it. In that lab network, students will have to discover, identify, and analyze the threat using active defense skills to guide incident responders to the affected Human Machine Interface (HMI).

- Students will learn effective tactics and tools to collect and preserve forensic-quality data in an ICS environment. Students will then use this data to perform timely forensic analysis and create IOCs.

- Students will learn how to analyze initial attack vectors such as spear-phishing emails, perform timely malware analysis techniques, analyze memory images, and create Indicators of Compromise in YARA. Students will analyze the malware, extract information, and develop YARA rules to complete the active defense model introduced in the class and maintain operations.

ISE 6525 (SANS Course ICS 456): Essentials for NERC Critical Infrastructure Protection | GCIP: GIAC Critical Infrastructure Protection:

- Students will develop an understanding of the electric sector regulatory structure and history as well as an appreciation for how the CIP Standards fit into the overall framework of the reliability standards. Key NERC terms and definitions related to NERC CIP are reviewed using realistic concepts and examples that prepare students to better understand their meaning. Students will explore multiple approaches to BES Cyber Asset identification and learn the critical role of strong management and governance controls, and will examine a series of architectures, strategies, and difficult compliance questions in a way that highlights the reliability and cybersecurity strengths of particular approaches.

- Students will learn practical implementations to consider and designs to avoid when employing firewalls, proxies, gateways, and IDS. Student will learn about the strengths and weaknesses of common physical controls and monitoring schemes.

- Students will understand CIP-007, with a focus on implementation examples and the associated compliance challenges, configuration change management, and vulnerability assessments that ensure systems are in a known state and under effective change control.

- Students will examine CIP-008 and CIP-009 covering identification, classification communication of incidents as well as the various roles and responsibilities needed in an incident response or a disaster recovery event.

- Students will learn the key components for running an effective CIP Compliance program. Students review the NERC processes for standards development, violation penalty determination, Requests For Interpretation, and recent changes stemming from the Reliability Assurance Initiative. Students will identify recurring and audit related processes that keep a CIP compliance program on track: culture of compliance, annual assessments, gap analysis, TFE's, and self-reporting. Students will understand how to prepare for NERC audits, and will analyze real-world CIP violations.

ISE 6715 (SANS Course AUD 507: Auditing and Monitoring Networks, Perimeters, and Systems | GSNA: Systems and Network Auditor

- Students will develop an understanding of the auditor's role in relation to policy creation and conformance, basic auditing and assessment strategies, effective risk assessment and root failure causes, the use of existing or new controls in the risk assessment process in physical and virtual environments, reporting of findings, contractual requirements, and hands-on audting using VMWare vSphere and ESXi.

- Students will understand how to employ or implement:
    - Secure Layer 2 configurations, including VLANs, spanning tree, network trunking, and switching fiber security;
    - Router & Switch Configuration Security, to include remote administration, logging concerns and practice, ACL configuration & validation, user management, and evolving technologies;
    - Firewall Auditing, Validation & Monitoring, to include information flow diagramming, converting requirements to ACLs, understanding firewall design, network architecture validation, rules review& analysis, technical validation of firewall rules, and next generation firewalls;
    - Wireless environments, including secure deployments and identification of wireless security issues;
    - Network Population Monitoring, to include robust processes for node identification, network population change management & monitoring, and automated notification processes;
    - Vulnerability Scanning

Each program learning outcome and course objective listed above is measured by the respective GIAC certification examination associated with each of the three courses that the student completes from those listed in Section G1, or by another appropriate and ongoing evaluation method for courses unique to STI which do not have an associated GIAC examination.

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

3. How General Education Requirements Will Be Met

As an graduate certificate program, the ICSS does not include general education requirements.

4. Specialized Accreditation/Certification Requirements

Each student who earns a ICSS graduate certificate will have achieved certification in at least three areas of cybersecurity using Global Information Assurance Certifications (GIAC).

H. Articulation

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

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

The faculty serving the students of the proposed ICSS program is comprised of the very same instructors who currently teach the 500+ enrolled graduate students at the SANS Technology Institute as well as the more than 30,000 professionals across the globe each year enrolled at SANS via live and online courses. Their qualifications to fulfill our mission were recently reviewed and confirmed by the Visiting Team of the Middle States Commission on Higher Education as part of STI's recent re-accreditation review. Adding 50 to 200 students (see Section L, Financial Resources) to the instructors' teaching load is the equivalent of far less than 1% increase in enrollment per class. Therefore, we conclude that our faculty is more than adequate in both capability and number to serve this new program.

Meeting STI's mission requires that STI faculty and graduates are "scholar-practitioners." STI uses the term "scholar-practitioner" to designate people who are both (1) highly trained professional practitioners focused on information security, and (2) scholars in the sense that they both contribute to and consume the research required to advance that professional practice. The combination enables them to incorporate new research into their work and create the new knowledge and solutions that others seek to use. Our faculty are not solely scholars, they must also be advanced practitioners of the subjects they teach so that they can show STI students how to practice security effectively. This gives STI students an advantage relative to graduates of other programs in which students learn theory, but not up-to-date practice. Finally, our faculty must be talented teachers, able to communicate often-difficult technical information in a clear and compelling manner.

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

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

- President Alan Paller was the Co-chair of the Department of Homeland Security's Task Force on CyberSkills, and had been a Charter Member of President Clinton's National Information Assurance Council.
- President Paller, Dr. Eric Cole, and James Lyne are three of fewer than 30 people currently listed on the Infosecurity Europe Hall of Fame.
- Dr. Johannes Ullrich was recognized as one of the 50 most powerful people in networking by NetworkWorld. Social media is replete with examples of references to SANS Instructors, including items like Security Leaders to Follow on Social Media.
- STI faculty are repeatedly invited to keynote presence at RSA, the industry's largest convocation for information security research and practice. For each of the last seven years, members of STI's faculty, led by President Alan Paller, have hosted one of the main keynotes at "RSA," focusing their presentation on their expectations for the seven most dangerous new attack techniques they expect to impact the industry in the subsequent year. The press release regarding the entire event issued by RSA is indicative of our faculty's prominence in the industry: not only are they one of the three keynotes highlighted (together with a Cryptographer's panel, which is the core activity of RSA), but they are presented prior to and in advance of the CEOs, Presidents, and leading executives from companies such as Microsoft, Hewlett Packard Enterprise, Symantec, Intel Security, and Cisco Security.
- STI faculty are sought after by the news media for their commentary on cybersecurity topics – STI faculty are frequently sought-after as commentators for breaking news articles on adverse cyber events. Their commentary appears in general news publications such as the New York Times and Wall Street Journal, in general magazines such as Forbes and Fortune, and their work is highlighted on various TV news programs. They are sought-after speakers even for general industry events, such as TED (James Lyne's February, 2013 TED talk on 'everyday cybercrime' has been viewed 1.5mm times).

As shown in Figure 1 (below), the SANS instructor development and assessment process requires a prospective STI faculty member to successfully complete four increasingly competitive steps (listed here and described in greater detail below):

(1) Earn scores on a Global Information Assurance Certification (GIAC) examination above 85.
(2) Earn high marks in mentoring (lab/teaching assistant) two groups of students.
(3) Earn high marks as "community instructors" in teaching two classes held at small Residential Institutes.
(4) Earn high marks as a supervised instructor at a large Residential Institute.

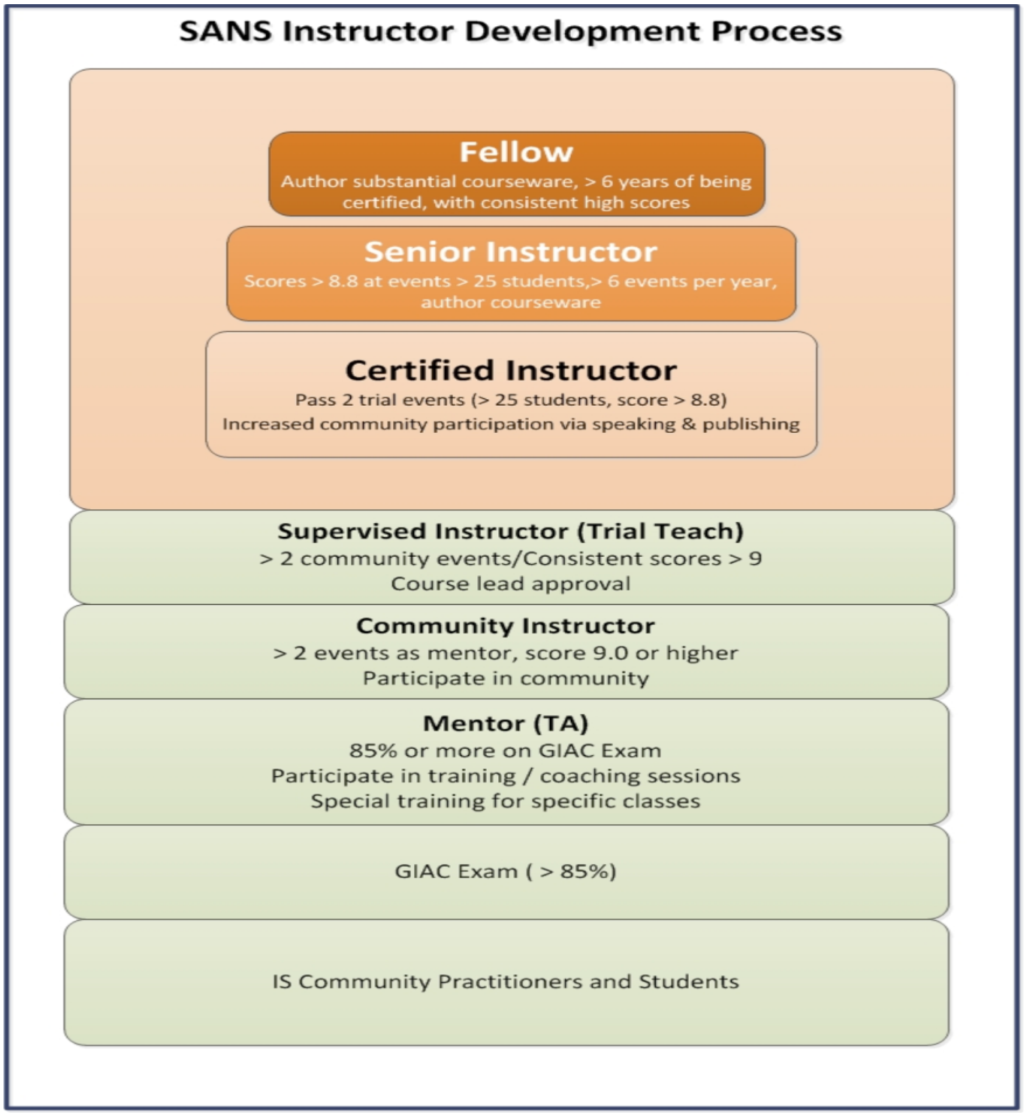
Only after completing these four steps would an individual would be eligible to be a SANS Certified Instructor and potentially be appointed to the STI faculty.

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

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

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

Figure 1 SANS Instructor Development and Assessment Process



SANS Instructor Development Process

Fellow
Author substantial courseware, > 6 years of being certified, with consistent high scores

Senior Instructor
Scores > 8.8 at events > 25 students,> 6 events per year, author courseware

Certified Instructor
Pass 2 trial events (> 25 students, score > 8.8)
Increased community participation via speaking & publishing

Supervised Instructor (Trial Teach)
> 2 community events/Consistent scores > 9
Course lead approval

Community Instructor
> 2 events as mentor, score 9.0 or higher
Participate in community

Mentor (TA)
85% or more on GIAC Exam
Participate in training / coaching sessions
Special training for specific classes

GIAC Exam (> 85%)

IS Community Practitioners and Students

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

Once appointed, qualified individuals serve in dual roles as SANS Instructors and STI faculty members. Each appointed instructor is a proven, real-world practitioner whose experiences are especially relevant to the school, enabling them to author courses of value, relevancy, and currency, as well as to deliver these courses to students in an effective, highly engaging manner that includes supplying ever-renewed examples from their work practice. These industry-recognized demarcations indicate technical achievement in the field, superior teaching effectiveness and student engagement as exemplified in the classroom and online, and successful completion of a competitive development process that employs both student and peer-faculty feedback to prove that the instructors possess these qualities.

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

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

Tim Conway

Tim Conway, besides being an instructor for ISE 6525, is the Curriculum Lead who is responsible for developing, reviewing, and implementing technical components of the SANS ICS and SCADA curriculum. Formerly, Tim was the Director of CIP Compliance and Operations Technology at Northern Indiana Public Service Company (NIPSCO), where he was responsible for Operations Technology, NERC CIP Compliance, and the NERC training environments for the operations departments within NIPSCO Electric. Previously, Tim was an EMS Computer Systems Engineer at NIPSCO for eight years, with responsibility over the control system servers and the supporting network infrastructure. He is the former Chair of the RFC CIPC, the current Chair of the NERC CIP Interpretation Drafting Team, a member of the NESCO advisory board, the current Chair of the NERC CIPC GridEx Working Group, and the Chair of the NBISE Smart Grid Cyber Security panel.

Robert M. Lee

SANS certified instructor Robert M. Lee brings to the classroom one of the most valuable and respected of credentials: real-world experience. Robert is the CEO and founder of his own company, Dragos, Inc., that provides cyber security solutions for industrial control system networks. Consider the 2015 attack on the Ukraine power grid when for the first time in history a power grid went down due to an intentional cyberattack. Robert and a few others formed a specialized team to analyze the event and passed information to the impacted parties as well as the U.S. government and private sector. He and his team also analyzed the malware from the 2016 cyber attack on Ukraine's Kiev substation and dubbed it CRASHOVERRIDE as the first ever malware tailored to specifically disrupt electric grid operations. Robert got his start in information security making small control systems for humanitarian missions. He joined the United States Air Force and became a cyberspace warfare operations officer in the U.S. intelligence community. In that role, he created and led a mission examining nation-states targeting ICS, the first mission of its kind in the U.S. intelligence community. Robert has a master's degree in cybersecurity and computer forensics from Utica College and a doctorate in war studies from King's College London. He was named one of Forbes' “30 under 30” in Enterprise Technology in 2016, was awarded EnergySec's 2015 Cyber Security Professional of the Year and named one of Passcode's "Influencers."

Matthew Luallen
Matthew Luallen is a well-respected information professional, researcher, instructor, and author. Mr. Luallen serves as the president and co-founder of CYBATI, a strategic and practical educational and consulting company. CYBATI provides critical infrastructure and control system cybersecurity consulting, education, and awareness. Prior to incorporating CYBATI, Mr. Luallen served as a co-founder of Encari and provided strategic guidance for Argonne National Laboratory, U.S. Department of Energy, within the Information Architecture and Cyber Security Program Office. In an effort to promote education and collaboration in information security, Mr. Luallen is an instructor and faculty member at several institutions. Mr. Luallen is adjunct faculty for DePaul University, teaching the Computer Information and Network Security Master’s degree capstone course. He is also a certified instructor and CCIE for Cisco Systems, covering security technologies, such as firewalls, intrusion prevention, and virtual private networks, and general secure information architecture. As a certified instructor for the SANS Institute, Mr. Luallen teaches infrastructure architecture, wireless security, web application security, regulatory and standards compliance, and security essentials. Mr. Luallen is a graduate of National Technological University with a master's degree in computer science, and he also holds a bachelor of science degree in industrial engineering from the University of Illinois, Urbana.

Billy Rios
Billy is an accomplished author and speaker. Billy is recognized as one of the world's most respected experts on emerging threats related to Industrial Control Systems (ICS), Critical Infrastructure (CI), and medical devices. He discovered thousands of security vulnerabilities in hardware and software supporting ICS and critical infrastructure. He has been publicly credited by the Department of Homeland Security (DHS) over 50 times for his support to the DHS ICS Cyber Emergency Response Team (ICS-CERT). Billy is the Founder of WhiteScope LLC which is known as a leading provider of deep security research, world class advisory services, and innovative security solutions. Prior to venturing into entrepreneurship, Billy served in a number of roles that demonstrated increasing responsibility and security expertise. As the Director of Vulnerability Research and Threat Intelligence with Qualys, Billy led the development of product offerings for vulnerability research, threat intelligence, ICS/SCADA, and embedded security. Before Qualys, Billy led the Google front-line response for externally reported security issues and incidents. Prior to Google, Billy was the Security Program Manager at Internet Explorer (Microsoft). During his time at Microsoft, Billy led the company's response for several high-profile incidents, including the response for Operation Aurora. Before Microsoft, Billy worked as a penetration tester, an intrusion detection analyst, and served as an active duty Marine Corps Officer. Billy currently holds an MBA from Texas A&M University-Commerce and a Master of Science in Information Systems from Hawaii Pacific University. He was a contributing author for several publications including: Hacking, the Next Generation (O'Reilly), Inside Cyber Warfare (O'Reilly), and The Virtual Battle Field (IOS Press).

Justin Searle
Justin Searle is a Managing Partner of UtiliSec, specializing in Smart Grid security architecture design and penetration testing. Justin led the Smart Grid Security Architecture group in the creation of NIST Interagency Report 7628 and played key roles in the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG). He currently leads the testing group at the National Electric Sector Cybersecurity Organization Resources (NESCOR). Justin has taught courses in hacking techniques, forensics, networking, and intrusion detection for multiple universities, corporations, and security conferences. Mr. Searle is currently a Senior instructor for the SANS Institute. In addition to electric power industry conferences, Justin frequently presents at top international security conferences such as Black Hat, DEFCON, OWASP, Nullcon, and AusCERT. Justin co-leads prominent open source projects including the Samurai Web Testing Framework (SamuraiWTF), the Samurai Security Testing Framework for Utilities (SamuraiSTFU), Middler, Yokoso!, and Laudanum. Justin has an MBA in International Technology and is a CISSP and SANS GIAC certified Incident Handler (GCIH), Intrusion Analyst (GCIA), and Web Application Penetration Tester (GWAPT).

A summary list of these ICSS graduate certificate faculty is available in Appendix 3.

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

<u>Ongoing Pedagogy Training for Faculty</u>:

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

The SANS development and continuous assessment process ensures that persons eventually chosen to teach STI students demonstrate (1) mastery in the community of practice in which they instruct, and (2) highly rated and effective teaching practices. An equally important element of teaching quality at STI is that SANS' ongoing assessment processes enable the college to ensure that teaching faculty retain both a high degree of technical mastery and outstanding teaching skills on an ongoing basis.

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

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

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

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

LMS and Distance Education Training for Faculty:

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

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

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

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

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

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

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

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

- Free and unlimited access to EBSCO's "Computers and Applied Sciences (Complete)" database. EBCSO is the leading provider of online research databases, e-journals, magazine subscriptions, e-books, and discovery services of all kinds. This full-text database covers computing, technology and engineering disciplines, and contains 650 active full-text journals and magazines, 520 active full-text peer-reviewed journals, 320 active full-text peer-reviewed journals with no embargo, and 410 active full-text and indexed journals.
- The SANS Security Policy Collection, which contains model security policies developed by major corporations and government agencies. The collection contains about 35 policies and grows as new security issues arise and policy templates are needed.
- The SANS Technology Institute's Cyber Research page, which provides access to exemplary graduate-level research papers, group projects, and presentations that cover a wide variety of topics of practical and academic relevance that have real-world impact and often provide cutting-edge advancements to the field of cybersecurity knowledge.
- The SANS Top-20 V7, a consensus list of vulnerabilities that require immediate remediation. The list is the result of a process that brought together dozens of leading security experts.
- The SANS Newsletter Collection, which helps keep students up to date with the high-level perspective of the latest security news.
- The Security Glossary, which is among the largest glossaries of security terms available on the Internet. It was developed jointly by SANS and the National Security Agency and provides authoritative definitions of many of the specialized terms students will encounter.
- The SANS Collection of Frequently Asked Questions about Intrusion Detection, available at contains 118 authoritative discussions of the primary topics that arise when planning and implementing intrusion detection technologies. The collection is available at http://www.sans.org/security-resources/idfaq/.
- The SANS Internet Storm Center Handler Diaries and Archives, which contain contemporaneous analyses of new attacks that are discovered on the Internet. The archives constitute an extraordinary research asset because of the depth of the analysis and the currency of the topics covered. They also provide SANS students with access to raw data, summaries, and query facilities to analyze malicious Internet traffic records. This is a rich data source for advanced security research projects that analyze attack patterns and how fast worms and other attacks spread through the Internet.
- SANS Web Briefings held several times a month that feature SANS faculty and other security experts providing up-to-date web briefings for SANS alumni on new threats seen at the Internet Storm Center, new technologies that are emerging, and analysis of security trends.

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

This program will be offered in combinations of three online modalities and in residential institutes. More than 400 residential institutes are available to ICSS students each year with a cumulative capacity of more than 40,000 students. Each year the residential program expands by 10 to 20 institutes. Thus, the proposed program will easily be accommodated in the existing in-person training programs. Currently scheduled live courses described in this curriculum can be found online here.

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

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

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

Table 1: RESOURCES

Resource Categories	Year 1	Year 2	Year 3	Year 4	Year 5
1. Reallocated Funds	0	0	0	0	0
2. Tuition/Fee Revenue (c + g below)	225000	480000	435000	472500	622500
a. Number of F/T Students	30	64	58	63	83
b. Annual Tuition/Fee Rate	7500	7500	7500	7500	7500
c. Total F/T Revenue (a x b)	225000	480000	435000	472500	622500
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	4.5	4.5	4.5	4.5	4.5
g. Total P/T Revenue (d x e x f)	0	0	0	0	0
3. Grants, Contracts & Other External Sources	0	0	0	0	0
4. Other Sources	0	0	0	0	0
TOTAL (Add 1 – 4)	225000	480000	435000	472500	622500

Table 2:
EXPENDITURES

Expenditure Categories	Year 1	Year 2	Year 3	Year 4	Year 5
1. Faculty (b + c below)	11250	24000	21750	23625	31125
a. # Sections offered	N/A	N/A	N/A	N/A	N/A
b. Total Salary	6750	14400	13050	14175	18675
c. Total Benefits	4500	9600	8700	9450	12450
2. Admin. Staff (b + c below)	16800	42000	42000	42000	58800
a. # FTE	0.2	0.5	0.5	0.5	0.7
b. Total Salary	12000	30000	30000	30000	42000
c. Total Benefits	4800	12000	12000	12000	16800
3. Support Staff (b + c below)	0	0	0	0	0
a. # FTE	0	0	0	0	0
b. Total Salary	0	0	0	0	0
c. Total Benefits	0	0	0	0	0
4. Equipment	0	0	0	0	0
5. Library	0	0	0	0	0
6. New or Renovated Space	0	0	0	0	0
7. Other Expenses	136750	222600	256950	305325	443325
TOTAL (Add 1 – 7)	164800	288600	320700	370950	533250

Finance Data: Narrative

Table 1: RESOURCES

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

2. Tuition and Fee Revenue
   Narrative: Describe the rationale for the enrollment projections used to calculate tuition and fee revenue.
   STI is currently recruiting 20-30 new graduate certificates per month, with not quite half of those typically going into our Penetration Testing program, about one quarter into our Incident Response program, and the remainder split roughly equally into the Cyber Defense and the Cyber Core programs. Thus, it is our more narrowly-focused graduate certificate programs which attract the greatest number of new students; however it is also true that penetration testing and

incident response are required functions across many industries, whereas this proposed program focuses into, if not one industry, then one vertical. Therefore, we use a conservative approach to projections for the above calculations.

The tuition projection for Year 1 assumes the ICSS program admits 30 full-time students during the course of the year, each of whom pay $5,000 per course. Currently, our graduate students complete an average of 1.5 courses per year, supporting an effective annual tuition of $7,500 per year per student.

In Year 2, we assume that the rate of admission to the program will admit 40 new students. As most of our graduate certificate students take roughly two years to complete their programs, this second year of growth is purely additive. Also, the two-year retention rate for graduate certificate students is generally about 80%. This retention rate is factored into the prior year's admitted number, and is added to the current year's admitted number to combine to a total number of students for that given year. Thus, the net total number students in year 2 is effectively 64.

For years 3, 4, and 5 we project 50, 60, and 75 new students per year. Applying the same logic presented above, this leads to a total effective student counts of 58, 63, and 83, respectively. We believe expectations for this growth growth are reasonable because we will be able to expand the offering of the program to students from other states via our online modalities.

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

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

5. Total Year
   Narrative: Additional explanation or comments as needed.

N/A

Table 2: EXPENDITURES

Faculty
ICS students may receive instruction live in-classroom or online, depending on the course and their own choices. When they attend live in-classroom, they join a class already being taught by STI faculty to other students, and the ICS students typically represent no more than a 5% - 10% increase in the total students in any given classroom. When they choose to take the course online, no additional faculty are required and, similar to live classes, ICS students represent only a small fraction of those students being taught by the existing group of subject-matter experts and teaching assistants and at any given time. Therefore, we do not anticipate any increase in the number of faculty required to teach ICS students, either live or online. In addition, the cost associated with the faculty and subject-matter experts/teaching assistants who teach these students is embedded into the payments associated with the Memorandum of Understanding between STI and SANS, at an effective rate of 5% of tuition revenue. Thus, for the sake of clarity, we have estimated a proportional cost for faculty salary and benefits as a percentage of total course load increase which is expected due to the creation of this new graduate certificate program.

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

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

Other Expenses
As described elsewhere, a core design element of the SANS Technology Institute are the Memoranda of Understanding signed with our parent, the SANS Institute, and a related entity, GIAC Corporation, that allow STI to select and pay for many costs on a variable, per-student basis. The ICS program will also benefit from this financial arrangement. The financial projections assume the same mix of payments that STI incurs today per student, as recently reviewed by the Middle States evaluation team during our re-accreditation study.

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

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

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

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

American National Standards Institute. GIAC exams increasingly include hands-on test questions where students can demonstrate they can use what they learned.

3. **To evaluate program outcomes,** STI tracks all graduates and asks them (and when possible, their employers) annually for feedback on how well the program worked for them and how it might be improved. Additionally, following its recent self-study and successful evaluation team visit, STI is implementing its formal Learning Outcomes Assessment Plan, as endorsed by the MSCHE evaluation team. Under this plan, each graduate certificate program undergoes a formal review by an evaluation team comprised of subject matter experts every four years. This review process will ensure alignment of (1) course outcomes to program learning objectives, of (2) program learning objectives to any capstone requirements, and of (3) both program learning objectives and capstone requirements to a survey of industry requirements.

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

TBD

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

Not applicable.

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

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

Appendix 1. Contracts with Related Entities

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

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

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

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

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

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

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

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

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

Purpose

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

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

Vision

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

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

Mission

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

Scope

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

Hours of Operations

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

Service Expectations

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

Accounting and Finance

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

Bursar & Registration

Process	**Service Expectation**	**Service Metric**

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

Human Resources

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

Marketing

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

Information Technology

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

Technical Course Maintenance & Presentation

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

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

Educational Residency

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

Service Constraints

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

Terms of Agreement

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

Periodic Quality Reviews

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

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

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

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

Service Level Maintenance

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

Issue Resolution

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

Payment Terms and Conditions

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

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

Agreed to on behalf of STI:

Eric A. Patterson
Executive Director
SANS Technology Institute

Agreed to on behalf of SANS:

Peggy Logue
Chief Financial Officer
SANS Institute

Date: Date:

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

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

RES 5900	N/A	$	0

SANS Technology Institute-GIAC Memorandum of Understanding

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

Contents

Purpose

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

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

Vision

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

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

Mission

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

Scope

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

Hours of Operations

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

Service Expectations

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

Service Constraints

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

Terms of Agreement

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

Periodic Quality Reviews

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

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

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

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

Service Level Maintenance

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

Issue Resolution

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

Payment Terms and Conditions

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

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

Agreed to on behalf of STI:

Eric A. Patterson
Executive Director
SANS Technology Institute

Date

Agreed to on behalf of GIAC:

Scott Cassity
Executive Director
GIAC

Date

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

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

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

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

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

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

(a) Curriculum and instruction

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

STI faculty members design all distance learning programs.

(b) Role and mission

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

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

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

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

(c) Faculty support

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

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

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

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

Instructor Guidelines for SANS Simulcast Classes

What to Expect

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

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

Advance Planning

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

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

Audio Tips

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

Starting Class

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

Teaching Tips

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

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

Suggested Best Practices

Jason Fossen:

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

Jason Lam:

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

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

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

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

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

- The SANS Information Security Reading Room contains more than 2,000 original research studies, not available from any other source, in 76 knowledge domains relevant to the study of information security. They are downloaded more than a million times each year. The Reading Room is available at http://www.sans.org/reading_room/.

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

(e) Students and student services

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Our ICS students will be upper division students, likely at least 19 years old, and well versed in information technology in order to have scored sufficiently high on CyberStart to gain acceptance. Thus, they have the needed background, knowledge, and technical skills to use the distance learning modalities.

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

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

(f) Commitment to support

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

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

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

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

(g) Evaluation and assessment

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

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

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

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

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

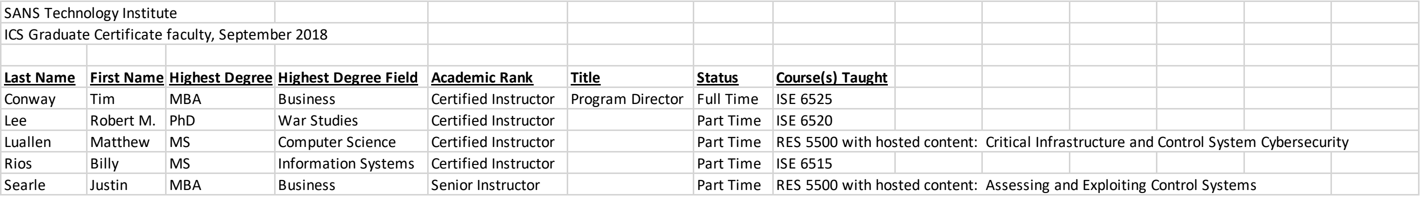
Ultimate student achievement in the ICS program will be measured by grades on the internationally standardized GIAC exams for each area of security. We compare these scores in distance and in-person learning modalities. As shown in Table A.4.3, the GIAC test scores in distance learning are essentially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

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

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

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

Appendix 3. Summary Listing of ICSS Graduate Certificate Faculty



SANS Technology Institute

ICS Graduate Certificate faculty, September 2018

Last Name	First Name	Highest Degree	Highest Degree Field	Academic Rank	Title	Status	Course(s) Taught
Conway	Tim	MBA	Business	Certified Instructor	Program Director	Full Time	ISE 6525
Lee	Robert M.	PhD	War Studies	Certified Instructor		Part Time	ISE 6520
Luallen	Matthew	MS	Computer Science	Certified Instructor		Part Time	RES 5500 with hosted content: Critical Infrastructure and Control System Cybersecurity
Rios	Billy	MS	Information Systems	Certified Instructor		Part Time	ISE 6515
Searle	Justin	MBA	Business	Senior Instructor		Part Time	RES 5500 with hosted content: Assessing and Exploiting Control Systems