SANS Technology Institute

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

Friday, May 25, 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,

It is with great enthusiasm that the SANS Technology Institute submits the attached proposal to create an Upper Division Certificate program in Applied Computer Security.

We believe that this program will provide Maryland students with a smooth, assured, and rapid pathway to high-paying jobs in critical technical roles in cybersecurity. Even before the program has been launched, 13 Maryland employers as well as employers from outside the state have expressed an interest in interviewing the students.

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

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

September 1, 2018

Projected Implementation Date

Upper Division Certificate	Applied Cyber Security
Award to be Offered	Title of Proposed Program
5199	11.1003
Suggested HEGIS Code	Suggested CIP Code
SANS Technology Institute	Ed Skoudis
Department of Proposed Program	Name of Department Head

Ed Skoudis	edskoudis@sans.edu	(908) 601-3234
Contact Name	Contact E-mail Address	Contact Phone Number

President/Chief Executive Approval

Signature and Date

5/23/18

Date Endorsed/Approved by Governing Board

SANS Technology
Institute

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

PROPOSAL FOR AN UPPER DIVISION CERTIFICATE IN APPLIED CYBER SECURITY

SANS Technology Institute

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 an Upper Division Certificate in Applied Cyber Security ("CACS"). Students in this program will work towards two outcomes: (1) proficiency in the fundamental technical knowledge and skills that serve as the baseline for all professionals in cybersecurity, and (2) early specialization in advanced skills that can be applied to particular areas of information security practice. The first outcome will be achieved by teaching students the fundamentals of the relevant underlying technologies, then providing them with the knowledge and skillsets to defend those technologies and to respond to the most typical attack vectors and incidents. The second outcome will be achieved by offering students an elective choice of one of six advanced courses covering topics such as monitoring and detection, network vulnerability testing, web application testing, network forensics, and industrial control systems security. Knowledge of the underlying technologies taught early in the program will be tested by typical exams and graded exercises, but student's mastery of the baseline and advanced technical topics will be validated by the applicable, nationally recognized certification examinations.

CACS students will complete three required courses and one elective course, earning three industry-recognized certifications:

Required Courses:		
Course	Assessment	Credits
ACS 2201: Technology Essentials	TechEssentials exam and graded exercises	3
ACS 3401: Security Essentials	GIAC Security Essentials certification exam (GSEC)	3
ACS 3504: Security Incident Handling and Hacker Exploits	GIAC Incident Handler certification exam (GCIH)	3
One Elective Course from the following:		
Course	Assessment	Credits
ACS 4508: Advanced Digital Forensics and Incident Response	GIAC Forensic Examiner certification exam (GCFE)	3
ACS 4410: Security Essentials for Industrial Control Systems	GIAC Industrial Cybersuecurity Professional exam (GICSP)	
ACS 4501: Advanced Enterprise Defender	GIAC Enterprise Defender certification exam (GCED)	
ACS 4503: Intrusion Detection In-Depth	GIAC Intrusion Analyst exam (GCIA)	
ACS 4542: Web App Pen Testing and Ethical Hacking	GIAC Penetration Tester exam (GPEN)	

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. The most common path will involve students taking the Security Essentials course live in a classroom setting with a cohort, while taking the other courses online from their homes. Students will have access to mentors and assistants online, interact with each other online and in pre-arranged meetings, submit a portion of their work for grading online, and take the three primary exams required to complete the courses live at a proctored testing center.

The CACS program is designed to complement and build upon the preparation students receive in Maryland community colleges, or in other undergraduate programs, and to prepare them for immediate employment. For admission to the CACS program, students must have completed at least 24 credit hours of college-level general education courses with a cumulative GPA of 3.0. Admission to the CACS program also requires students to have achieved a score of a least 20,000 (subject to adjustment) on the then-current version of the CyberStart Game, the educational simulation program that measures aptitude for cybersecurity mastery.

2. Relation to STI Mission and Strategic Goals

The mission of the SANS Technology Institute states that we "develop technically-skilled leaders to strengthen enterprise and global information security." Our Vision Statement asserts that we seek to be the pre-eminent institution "translating contemporary information security practice and scholarship into effective educational experiences."

The proposed upper division certificate program not only aligns with STI's mission and vision, but is also core to accomplishing them.

The first and most critical of STI's four goals in its 2017–2021 Strategic Plan is to "materially increase the number of graduates prepared to lead cybersecurity teams, programs, and efforts." We have had success in producing graduates of the master's program who are making a profound difference in the cybersecurity posture of the organizations where they work, as documented in our Middle States' Self-Study Report prepared for the recently completed Team Visit Report to the Commission on Higher Education, and further recognized in the visiting team chair's report on that visit.

However, we are not having sufficient impact because we are not teaching enough students. Nearly every STI master's degree student is employed full-time and most have families. Our graduate courses are challenging and take a great deal of time (at least 10 hours per week for at least 3½ years) to master at a level that enables students to pass the rigorous, required certification exams.

We believe that creating a new program for undergraduate students comprised of courses that develop a core set of baseline knowledge and capabilities will provide two benefits. First, it will increase the number of individuals entering the cybersecurity workforce with hands-on mastery of the foundations of cybersecurity. Second, it will provide a continuing pipeline of people who, after two to five years of successful technical contributions as employees of corporations and government agencies in cybersecurity roles, and after completion of their BS degree, may come back to STI to earn the Master of Science in Information Security Engineering. This will enable them to become Technical Directors and CISOs adequately prepared to profoundly improve cybersecurity in their organizations, and help STI meet its primary strategic goal of increasing the number of master's degree graduates who can be technical leaders.

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

1. Critical Need for the CACS Program

Admiral Mike Rogers, Commander of U.S. Cyber Command and Director of the National Security Agency (NSA), told the U.S. Congress in May 2017, "Every conflict around the world now has a cyber dimension. Cyber war is not some future concept or cinematic spectacle; it is real and here to stay." There has been widespread discussion of the need for high-performing professionals to enable the United States to prevail in such conflicts, both in the military and in protecting critical infrastructure and other non-military entities. What is not so widely discussed is the extreme need for more people with hands-on advanced technical skills in specific roles in cybersecurity. Two seminal studies have documented the need for programs like the CACS program:

> (1) A report by the DHS Task Force on Cyber Skills established by the Secretary of the Department of Homeland Security concluded that, to meet the nation's critical cyber manpower needs, the government should focus on education programs comprised of "courses with hands-on components and frequent testing that ensure actual mastery of the knowledge and skills." It found that few NSA-designated Centers of Academic Excellence (primarily only those colleges designated as CAE-Cyber Operations programs) are graduating significant numbers of people with the hands-on technical skills needed by the nation. The report also isolated 10 "Red-Zone" jobs that the Task Force said were the most critically needed by the nation. Each STI CACS graduate will have earned certification in at least 2 of those 10 critical roles.
>
> (2) A report by the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency concluded: "A critical element of a robust cybersecurity strategy is having the right people at every level to identify, build and staff the defenses and responses. And that is, by many accounts, the area where [the United States is] the weakest." The commission, which was chaired by a U.S. senator and a U.S. congressman, made two key recommendations: promote and fund the development of more rigorous curricula in our schools; and support the development and adoption of technically rigorous professional certifications that include a challenging educational and practical component.

The demand from Maryland employers for people with the knowledge and hands-on skills that will be developed in the CACS program, and the demand from Maryland students for education that ensures they learn these hands-on skills, were both demonstrated in the first quarter of 2018. When SANS (the parent of STI) announced the availability in January 2018 of 80 places in a non-credit program that includes the two basic course and certification pairs of the CACS degree, 13 Maryland employers participated in the announcement and allowed SANS to include their logos in the program roll-out (see graphic with logos). These employers have been interviewing candidates prior to their acceptance into the SANS program and providing recommendations so that SANS can have confidence that students who are accepted are employable and likely to be hired immediately upon completing the program. Employer interviews will carry over to the CACS program: Appendix 1 includes letters from these employers expressing interest in hiring students with the certifications developed in the CACS program.

Employer Partners
CACI
EVER VIGILANT
RBR-TECHNOLOGIES
ALTA
IT Services
PLEX
Spry
HALFAKER
CONTINUING TO SERVE
Aerstone
NTTSecurity
DATAPRISE
GEICO
ThermoFisher
SCIENTIFIC
IntelliDyne
DEFENSE POINT
SECURITY

Equally important, the response to the announcement by applicants demonstrated student demand for such programs. In the first 68 days after the program was announced, 320 Marylanders applied, and approximately 8 more are applying each week as this application is being drafted. SANS limited applications by saying the program was for veterans and women, so the 320 applications in 68 days may significantly underestimate student demand for the program.

Maryland has the highest concentration of intelligence and military organizations with missions involving cybersecurity. World-class cyber skills are central to accomplishing those missions. Thus, it is appropriate that Maryland lead the nation in fostering educational programs that produce graduates who impress those employers with the depth of their preparation and the value they can bring to the job from the first day.

Eliminating the gap between employer needs and college cybersecurity programs is a core national imperative that must be met if our nation hopes to protect our Internet-dependent economy, our fully automated power and other critical infrastructure, and our computer-based, networked weapon systems. The three courses and certifications students can earn in the CACS program have proven they can teach the skills needed to close that gap.

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

New partnerships between colleges and businesses

The proposed program provides an innovative mechanism to implement Strategy 8 of the Maryland State Plan, which states: "Develop new partnerships between colleges and businesses to support workforce development and improve workforce readiness." Specifically, it develops job-ready graduates to fill high-paying jobs offered by Maryland employers that have partnered with STI to help ensure the success of students. The corporations are not just being magnanimous. They need hands-on mastery of applied cybersecurity skills that they believe they can only get through programs that ensure that students pass rigorous certification exams prior to graduation. They pay for their existing employees to earn those certifications, so they are aware of the level of deep mastery and subsequent job success associated with those credentials. They are supporting STI in establishing an undergraduate curriculum that leads to those highly valued credentials because they feel they waste too much time and money retraining employees who, in the employers' view, should have come to them from colleges more job-ready. In sum, the CACS provides a powerful test of a skills-development and industry certification-based undergraduate credential in Maryland.

Increase student success with less debt

The CACS program will address the State Plan's goals to increase student success with less debt. We strongly believe, even though CACS will be more expensive per credit hour than most college programs focused on developing cybersecurity skills, that our graduates will have greater job placement success and earn higher salaries after a program whose total cost reflects only 15 credit hours, relative to those that need to pay for another 60 credit hours to earn a bachelor's but who wouldn't at that point possess three industry-respected certifications that can justify a hiring decision or command a higher starting salary.

More specifically, however, STI intends to provide students with two innovative options that can effectively "finance" their CACS studies, align our interests, and reduce the risk of unnecessary debt burdens:

- First, students may confidently choose to use Title IV funding because STI will guarantee that if the student seeks but does not find a full-time job with total compensation exceeding $65,000 per year within two years, STI will repay all of the student's remaining debt associated with the CACS program.
- Second, each student accepted into the program will have the option to elect in advance to pay us by allocating 10% of their compensation from any job they take after they graduate from the CACS program for three years.

These options will be available in addition to others that do not impose a debt burden, including veteran's benefits, Pell Grants, or, for those who are already employed, employer tuition reimbursement benefits or training stipends. By providing all of these options, STI seeks to align our admissions choices and investments with actual (and not just intended or promised) student success, and allow prospective students to seek and achieve that success with less debt.

The CACS program also targets elements of two other Strategies in the Maryland State Plan. Strategy 7 calls for special efforts to support veterans. Since 2015, SANS has operated a support program for veterans, and our students who are veterans are having success in the challenging courses and certifications, and are being hired at defense-oriented and other organizations that honor their sacrifice as well as their skill. Here's how Chief Master Sgt. Alexander Hall, 50th Network Operations Group Superintendent, U.S. Air Force, described the program in an article published in 2014 by the public affairs office of Schriever AFB, CO, supporting Defensive Cyberspace Operations for Air Force Space Command:

> We found Air Force IT personnel who were either separating or retiring, had certain levels of education or experience and who would be strong candidates. Finding approximately 600 people, we mailed them saying, "We know you're leaving the Air Force soon, are you interested in giving this [program] a shot? [There's] no cost to you, and if you're successful, you're going to get a job."
>
> The first pilot group to spearhead VetSuccess was assembled – nine Airmen in total. All passed with flying colors. The success of VetSuccess has only flourished to this day. During the last training cohort, every successful participant was negotiating for jobs making $70,000 to $120,000, just four months after leaving the service. To date, more than 80 veterans have been trained and taken valuable cybersecurity jobs.
>
> We know that IT veterans have all the things that the industry wants, what we're missing though, is the opportunity to put ourselves on display. That's what VetSuccess allows us to do; we go through industry standard training and certification to show ourselves off. Through this training we have proven that we know everything that our civilian counterparts know, and the IT industry is ready to hire us now.

And here's how one VetSuccess graduate described the program's impact on his life:

> "Completing the SANS VetSuccess Academy not only influenced my career plans, it defined them. The education and certifications opened doors that were inaccessible to me otherwise, short of winning the lottery. In fact, being selected into the inaugural cohort was a 'hitting the jackpot' moment for me."
>
> - Retired USAF SMSgt Ed Russell, now employed at NTT Security

The CACS program would eliminate a major barrier and enable STI to do much more for veterans. Many veterans enroll in STI graduate certificates to master SANS material and make use of their VA education benefits. However, a substantial number of candidates are not eligible for admission to our graduate programs because they have not completed a four-year degree. The upper division CACS program, offered by a regionally accredited institution, would provide a pathway for many previously ineligible veterans to take advantage of STI VA-eligible programs to earn advanced cybersecurity credentials and get the higher-paying jobs for which those certifications qualify them.

Finally, Strategy 4 of the Maryland State Plan calls for collaboration between historically black universities and colleges (HBCUs) and other institutions to ensure equal educational opportunity for all Marylanders. SANS has optimized a cyber talent identification game that allows people who have never worked in IT to discover whether they would be good at cybersecurity and whether they would like it. We will make the same game available to students in HBCUs that choose to be partners, and we will follow up with additional support for the HBCUs to help their talented students pursue further study in cybersecurity and its foundations.

The effectiveness of the talent identification game was demonstrated in January-February 2018 when Governor Larry Hogan partnered with SANS on a version of it entitled the GirlsGoCyberStart Program. The results: 404 Maryland high school girls signed up in 18 days. Maryland teams took 4 of the top 6 places among 2,700 teams from 17 states. The key takeaway was that many young women who thought they would not be any good at cybersecurity are now interested in exploring a career in the field. The fraction of young women interested in a STEM/cybersecurity career grew from 35.6% before the girls played to 69.8% after they played.

Towards an overall goal of increasing student success, SANS will also make the talent identification game available to students in every one of the 16 Maryland community colleges that want to partner with SANS to open the door for talented students to discover their talent and be discovered as people who can make a difference in cybersecurity through the STI CACS program.

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

1. Market Demand

The National Institute of Standards and Technology (NIST) supports a website of data on cybersecurity jobs called CyberSeek that lists the number of current job openings by state and metropolitan area. In this section we combine the CyberSeek data with employment projections from the Maryland Department of Labor Licensing and Regulation (DLLR) to estimate the demand for the STI CACS program in Maryland and in the region.

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

CyberSeek lists eight "top cybersecurity job titles" that are shown in Table 1 along with numbers of people in Maryland holding those jobs in 2014 and projected growth in demand for those jobs up to 2024. Clearly, not all these jobs can be called cybersecurity jobs. Yet, it is difficult to be hired into any of them without demonstrating a substantial knowledge of cybersecurity vulnerabilities and attack vectors that could disable the systems, networks, or software an employee will be developing or managing. Moreover, deep knowledge of hands-on cybersecurity like that gained in the CACS program can be a strong indicator of potential for rapid advancement and therefore a good reason to hire a candidate into any of these roles instead of other candidates who do not have the GIAC certifications earned by CACS students.

Table 1. Current Positions and Growth Projected Growth to 2024 in CyberSeek's "Top Cybersecurity Job Titles"

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

Source: http://www.dllr.state.md.us/lmi/iandoproj/maryland.shtml (accessed 4/2/18).

CyberSeek estimates the number of current cybersecurity job openings in Maryland at 14,535, which is not inconsistent with the DLLR numbers. However, the number of current job openings substantially underestimates demand for the CACS program. People who are already employed in entry-level cybersecurity roles will also be drawn to the program because many of them have had no previous opportunity to develop the advanced skills or to pass the GIAC exams offered through the proposed program. They may apply to STI because they are excited about the added contribution they could make with these skills, or because they may see a wave of more highly skilled job candidates coming and want to stay ahead of the new employees.

In sum, we foresee strong demand among students of a least 1,000 per year for the new CACS certificate, and we have shown evidence that those graduates are likely to be hired by eager employers, and that employers may sponsor CACS certificates for their current employees.

2. Current and Projected Supply of Prospective Graduates

Three upper division certificate programs focused on cybersecurity are listed in the Maryland Higher Education Commission Secure Data Web Degree Trend data summarizing degrees granted by Maryland institutions, detailed in Table 2.

Table 2. Upper Division Certificate Programs in Cybersecurity in Maryland

School Name	Degree Level	Program Name	CIP	Add/ Discontinue	Degrees 2012–2016
Univ. of MD University College	Upper Division Certificate	Information Assurance	111003	Discontinued in 2012	82
Univ. of MD University College	Upper Division Certificate	Security Operations	439999	Discontinued in 2012	0
Capitol Technology University	Upper Division Certificate	Computer and Network Security	110101	Approved in 2001	13

The two upper division certificate programs at the University of Maryland University College were discontinued in 2012, and the third, at Capitol Technology University, has granted only 13 certificates in the past five years, including four in 2016, the last year reported.

Two other types of undergraduate programs that are beyond associate's degrees but still at the bachelor's level seek to prepare people for cybersecurity roles: bachelor's degrees specifically in cybersecurity, and cybersecurity specializations within a BS computer science degree program. Table 3 shows the Maryland Higher Education Commission Secure Data Web Degree Trend data summarizing degrees granted by all bachelor-level programs in cyber, computer, or information systems security in Maryland over 2012 to 2016.

Table 3. Bachelor Degree Programs in Cybersecurity in Maryland

School Name	Degree Level	PGM-CD	Program Name	CIP	Degrees Granted 2012–2016
Capitol Technology University	Bachelors	70116	Cyber and Information Security	119999	70
Frostburg State University	Bachelors	70210	Secure Computing & Info Assurance	111003	6
ITT Technical Institute	Bachelors	70200	Information Systems Security	111003	0
Univ. Of MD University College	Bachelors	70204	Computer Networks & Security	110401	1556
Univ. Of MD University College	Bachelors	70210	Cyber Security	111003	1586

Another pathway for undergraduate students to prepare for jobs in cybersecurity is to enroll in a cybersecurity specialization within a computer science degree program. The Maryland Higher Education Commission Secure Data Web Degree Trend site shows 24 computer science bachelor programs in Maryland. Table 4 lists those programs and shows, by shading, the six computer science bachelor's degree programs that offer, according to their computer science web page, a specialization in cybersecurity with a program of required courses or a concentration in cybersecurity without a required course of study.

Table 4. Bachelor Degree Programs in Computer Science in Maryland with and without Specializations in Cybersecurity

School Name	Degree Level	Program Name	Degrees Granted, 2012–2016	Specialization in Cyber
Univ. of MD, College Park	Bachelors	Computer Science	1183	Yes
Univ. of MD, Baltimore County	Bachelors	Computer Science	604	Concentration
Univ. of MD University College	Bachelors	Computer Science	570	No
Towson University	Bachelors	Computer Science	316	Yes
Stevenson University	Bachelors	Computer Information Systems	243	Yes - forensics
Johns Hopkins University	Bachelors	Computer Science	170	Yes
Salisbury University	Bachelors	Computer Science	94	No
St. Mary's College of Maryland	Bachelors	Computer Science	87	No
Frostburg State University	Bachelors	Computer Science	80	No
Hood College	Bachelors	Computer Science	60	No
Univ. of MD Eastern Shore	Bachelors	Computer Science/Data Processing	55	No
Bowie State University	Bachelors	Computer Science	50	Yes
Morgan State University	Bachelors	Computer Science	42	No
Loyola University Maryland	Bachelors	Computer Science	37	No
McDaniel College	Bachelors	Computer Science	33	No

Frostburg State University	Bachelors	Computer Information Systems	29	No
Washington College	Bachelors	Computer Science	26	No
Mount St. Mary's University	Bachelors	Computer Science	24	No
Coppin State University	Bachelors	Computer Science	23	No
Capitol Technology University	Bachelors	Computer Science	23	No
Goucher College	Bachelors	Computer Science	17	No
Notre Dame of Maryland University	Bachelors	Computer Information Systems	11	No
Washington Adventist University	Bachelors	Computer Science	5	No
Notre Dame of Maryland University	Bachelors	Computer Science	0	No

No data have been published on the number of students earning computer science degrees with specializations in cybersecurity. Our belief is that the number of job openings for employees with substantial hands-on mastery of advanced topics in cybersecurity – as demonstrated by their passing rigorous, nationally standardized certification exams – is substantially greater than the number of graduates with those skills being produced by the three types of programs listed in this section. That conclusion is supported by the employers' letters of support and student demand for places in the SANS nondegree program. As noted above, there is substantial demand from employers and students alike for a program like the CACS, where students prove their mastery of three advanced topics in cybersecurity by passing widely used certification exams. For emphasis, we repeat the passage from Section B1 above:

> *When SANS (the parent of STI) announced the availability of 80 places in a non-credit program that includes the two basic course and certification pairs of the CACS degree in January 2018, 13 Maryland employers participated in the announcement and allowed SANS to include their logos in the program roll-out. These employers have been interviewing candidates prior to their acceptance into the SANS program and providing recommendations so that SANS can have confidence that students who are accepted are employable and likely to be hired immediately upon completing the program.*
>
> *Equally important, the response to the announcement by applicants demonstrated student demand for such programs. In the first 68 days after the program was announced, 320 Marylanders applied, and approximately 8 more are applying weekly as this application is being drafted. We limited applications by saying the program was for veterans and women, so the 320 applications in 68 days may significantly underestimate student demand for the program.*

D. Reasonableness of Program Duplication

1. Similarities and Differences between the CACS 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 CACS program is not unreasonably duplicative, and that it is an important addition to the educational offering in Maryland.

Degree to Be Awarded

As documented in the previous section, using Maryland Higher Education Commission data, only Capitol Technology University currently offers an Upper Division Certificate in Computer and Network Security, and that program awarded only four certificates in 2016, the last year reported. The two other Maryland Upper Division Certificate programs that focused on cybersecurity were discontinued in 2012. The demand for cybersecurity workers far exceeds the number of programs that are designed, at the upper division certificate level, to supply that demand.

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 CACS program will hold three industry-recognized GIAC certifications in addition to their upper division 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 CACS 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 CACS program also enables students to choose between a semester-based program or a more flexible year-long program that allows students to work a full-time job while they complete the program.

Role and Mission

Cybersecurity education is the sole focus of STI's mission. Furthermore, we offer students several unique payment options that are unparalleled at other schools: (1) We will forgive any tuition debt of a graduate who doesn't get a full-time job with compensation over $65,000 within two years after graduation; (2) We allow students to choose to pay us by allocating 10% of their compensation to us over the three years after they graduate from the program; and (3) We will reduce the tuition owed to us by the student by the amount of payments we receive from any employer that pays us a "recruiting fee" should we introduce them to, and they proceed to hire, that graduate. Our financing options are a direct result of our mission, and are a uniquely valuable element of our offering.

Admissions Requirements

STI's admission requirements for CACS include a score of at least 20,000 (subject to review and adjustment) on the then-current version of CyberStart, a requirement not used by any other college in Maryland. CyberStart is a program variously called a course, a game, an aptitude test, a talent discovery system, and a simulator. It is remarkably effective in identifying people with talent for excellence in cybersecurity, even those who had no idea that they had that talent. The United Kingdom adopted CyberStart as the core of its $25 million HMG CyberDiscovery Programme launched in November 2017 to find candidates to be developed into elite cybersecurity analysts for the UK military and intelligence community as well as other employers.

The 20,000 score was achieved by 12% of high school girls who signed up for Governor Hogan's GirlsGoCyberStart initiative in February 2018.

By accepting students who have demonstrated outstanding natural talent through CyberStart, STI can accelerate the student learning process by enabling a focus on academic content and competencies. This differentiates the CACS from the cybersecurity degree programs and other programs listed in Section D1 above because it involves mastery prior to graduation of three professional cybersecurity certifications that are widely recognized and valued by employers, and that make graduates immediately job ready.

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 CACS program has no impact on the uniqueness or identity of any of the HBIs.

However, on a more important level, since STI has the resources, we should have an impact in the HBIs in finding and assisting minority students with natural aptitude to excel in cybersecurity.

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

1. Program Outline and Requirements

Required Courses

ACS 2201: Technology Essentials (3 credits)

ACS 2201 is purpose-built to teach a baseline understanding of the fundamental technologies that underpin and define cybersecurity, and that serves as a preparatory step for ACS 3401. Regardless of their individual starting points, students will develop required knowledge of topics ranging from the architecture of modern computers to topics spanning how a CPU works, at a level that enables students to understand how malicious actors can suborn CPU processes, including the addressing of memory and the relationships between hardware and operating systems. It similarly covers networking and network protocols, Linux, Python programming, and other foundational topics. The goal is not for students to be expert in these technologies, but rather to be able to understand and have hands-on engagement with them to a degree sufficient for the practice of information security.

Through an online platform, students in this course engage in more than 40 hours of "seat time" augmented with labs, quizzes, Q&A with instructors, and ample outside work that reinforces the concepts taught. Instructional modules are stacked so that concepts are progressively built up and a detailed understanding is developed. Students study a diverse set of topics that slowly increase in difficulty until they grasp each concept, rather than overloading them with information on a single topic. Students with little background are able to move at a slower pace in earlier modules and levels of the simulation, while students who have some related understanding will complete earlier modules quickly and move on to topics they don't already know.

The online platform also features web-based access to virtualized labs, enabling students to get hands-on practice with Linux commands and to solve security problems without the difficulty of setting up infrastructure. This significantly reduces the barrier to entry and allows for transition from theory to hands-on exercises for a more engaging student experience.

ACS 2201 also teaches logic, programming and scripting and introduces how each of these can lead to errors that allow security experts or cyber criminals to find faults and exploit them.

Assessments: Forty-six quizzes and forty-six exams throughout the course plus an examination covering the full course.

ACS 3401: Security Essentials (3 credits)

ACS 3401is the CACS introductory, technically oriented course in information security. It establishes the foundations for designing, building, maintaining, and assessing security functions at the end-user, network, and enterprise levels of an organization. This course will prepare students to design and build a network architecture using VLANs, NAC, and 802.1x based on an APT indicator of compromise; run Windows command line tools to analyze the system looking for high-risk items; run Linux command line tools (ps, ls, netstat, etc.) and basic scripting to automate the running of programs to perform continuous monitoring of various tools; install VMWare and create virtual machines to operate a virtual lab to test and evaluate the tools/security of systems; create an effective policy that can be enforced within an organization and prepare a checklist to validate security, creating metrics to tie into training and awareness; and identify visible weaknesses of a system using various tools including dumpsec and OpenVAS, and once vulnerabilities are discovered cover ways to configure the system to be more secure. ACS 3401 is an extended version of SANS Course 401, tailored to the CACS program and adding significant time and exercises for mastering the underlying foundations on which successful technical cybersecurity careers are built.

Assessment: GIAC Security Essentials Certification (GSEC) examination

ACS 3504: Incident Handling and Hacker Exploits (3 credits)

By adopting the viewpoint of a hacker, ACS 3504 provides an in-depth focus into the critical activity of incident handling. Students are taught how to manage intrusions by first looking at the techniques used by attackers to exploit a system. Students learn responses to those techniques, which can be adopted within the framework of the incident handling process to handle attacks in an organized way. The faculty instruction, lab exercises, and exam are coordinated to develop and test a student's ability to utilize the core capabilities required for incident handling. Students will learn to apply incident handling processes – including preparation, identification, containment, eradication, and recovery – in order to protect enterprise environments; analyze the structure of common attack techniques to evaluate an attacker's spread through a system and network, anticipating and thwarting further attacker activity; use tools and evidence to determine the kind of malware used in an attack, including rootkits, backdoors, and Trojan horses, choosing appropriate defenses and response tactics for each; use built-in command-line tools such as Windows tasklist, wmic, and reg, as well as Linux netstat, ps, and lsof, to detect an attacker's presence on a machine; analyze router and system ARP tables along with switch CAM tables to track an attacker's activity through a network and identify a suspect; use memory dumps and memory analysis tools to determine an attacker's activities on a machine, the malware installed, and other machines the attacker used as pivot points across the network; gain access to a target machine using Metasploit, and then detecting the artifacts and impact of exploitation through process, file, memory, and log analysis; analyze a system to see how attackers use the malware to move files, create backdoors, and build relays through a target environment; run the Nmap port scanner and Nessus vulnerability scanner to find openings on target systems, and apply tools such as tcpdump and netstat to detect and analyze the impact of the scanning activity; apply the tcpdump sniffer to analyze network traffic generated by a covert backdoor to determine an attacker's tactics; employ the netstat and Isof tools to diagnose specific types of traffic-flooding denial-of-service techniques, and choose appropriate response actions based on each attacker's flood technique; and analyze shell history files to find compromised machines, attacker-controlled accounts, sniffers, and backdoors. This course is an extended version of SANS Course SEC504, adding extensive study of actual attacks and a student project to develop a profile of a major attack, present it to the community through a YouTube video, and evaluate other students' attack profile presentations.

Assessment: GIAC Certified Incident Handler (GCIH) examination

Electives Courses: Choice of One

ACS 4508: Advanced Digital Forensics and Incident Response (3 credits)

Incident response tactics and procedures have evolved rapidly over the past few years. Data breaches and intrusions are growing more complex. Adversaries are no longer compromising one or two systems in an enterprise – they are compromising hundreds. A team can no longer afford antiquated incident response techniques, it must identify compromised systems quickly, provide effective containment of the breach, and rapidly remediate the incident. This in-depth, digital forensics course provides responders with advanced skills to hunt down, counter, and recover from a wide range of threats within enterprise networks. Situations include APT adversaries, organized crime syndicates, and hactivism. Students will learn advanced use of a wide range of best-of-breed, open-source tools in the SIFT Workstation to perform incident response and digital forensics; how to hunt and respond to advanced adversaries such as nation-state actors, organized crime, and hacktivists; threat hunting techniques that will aid in quicker identification of breaches; rapid incident response analysis and breach assessment; incident response and intrusion forensics methodology; remote and enterprise incident response system analysis; Windows live incident response; memory analysis during incident response and threat hunting; detailed instruction on Windows enterprise credentials and how they are compromised; internal lateral movement analysis and detection; rapid and deep-dive timeline creation and analysis; volume shadow copy exploitation for hunting threats and incident response; detection of anti-forensics and adversary hiding techniques; discovery of unknown malware on a system; adversary threat intelligence development, indicators of compromise, and usage; cyber-kill chain strategies; and step-by-step tactics and procedures to respond to and investigate intrusion cases. Constantly updated ACS 4508 addresses today's incidents by providing hands-on forensics tactics and techniques that elite responders are successfully using in real-world breach cases. ACS 4508 is a substantially extended version of SANS Course FOR508, adding in-depth systems and networking knowledge that make a good forensics analyst an even better one.

Assessment: GIAC Certified Forensic Analyst (GCFA) examination

ACS 4410: Security Essentials for Industrial Control Systems (3 credits)

With the dynamic nature of industrial control systems (ICS), many engineers do not fully understand the features and risks of many devices. For their part, IT support personnel who provide the communications paths and network defenses do not always grasp systems' operational drivers and constraints. This course is designed to help traditional IT personnel fully understand the design principles underlying control systems and how to support those systems in a manner that ensures availability and integrity. In parallel, the course addresses the need for control system engineers and operators to better understand the important role they play in cybersecurity. This starts by ensuring that a control system is designed and engineered with cybersecurity built into it, and that cybersecurity has the same level of focus as system reliability throughout the system lifecycle. Students will gain an understanding of ICS components, purposes, deployments, significant drivers, and constraints; use hands-on lab learning experiences to control system attack surfaces, methods, and tools; learn control system approaches to system and network defense architectures and techniques; learn incident-response skills in a control system environment; learn governance models and resources for industrial cybersecurity professionals; and gain an appreciation, understanding, and common language that enables them to work together to secure ICS environments. The course helps develop cyber-secure-aware engineering practices and real-time control system IT/OT support carried out by professionals who understand the physical effects of actions in the cyber world. This course is an extended version of SANS Course ICS410, adding extensive operating system, networking, hardware, and common exploit modules that will make the IT people much stronger partners for ICS engineers.

Assessment: Certified Industrial Cybersecurity Professional (GICSP) examination

ACS 4501: Enterprise Defender (3 credits)

Many students call this the "Greatest Hits" course because it brings together all the elements of a modern cyber defense program. Students learn how to identify threats and build defensible networks to minimize the impact of an attack, use tools to detect adversaries, decode and analyze packets using various tools to identify anomalies, understand how adversaries compromise networks, perform penetration testing against their own organization to find vulnerabilities, apply the six-step incident response plan, use tools to remediate malware infections, and create a data classification program to make data loss protection systems effective. This is an extension of SANS Course SEC501, adding in-depth learning exercises covering networking, common attack techniques, and Linux.

Assessment: Certified Enterprise Defender (GCED) examination

ACS 4503: Intrusion Detection In-Depth (3 credits)

ASC 4503 delivers the technical knowledge, insight, and hands-on training needed to defend networks with confidence. Students will learn about the underlying theory of TCP/IP and the most used application protocols, such as DNS and HTTP, so that they can intelligently examine network traffic for signs of an intrusion. Students will get plenty of hands-on practice learning to configure and run open-source Snort, and write Snort signatures; configure and run open-source Bro to provide a hybrid traffic analysis framework; understand TCP/IP component layers to identify normal and abnormal traffic; use open-source traffic analysis tools to identify signs of an intrusion; comprehend the need to employ network forensics to investigate traffic to identify a possible intrusion; use Wireshark to carve out suspicious file attachments; write tcpdump filters to selectively examine a particular traffic trait; craft packets with Scapy; use the open-source network flow tool SiLK to find network behavior anomalies; and use knowledge of network architecture and hardware to customize placement of IDS sensors and sniff traffic off the wire. Daily hands-on exercises suitable for all experience levels reinforce the course book material so that students can transfer knowledge to execution. This course is an extended version of SANS Course SEC503, with significant additional hands-on problem-solving time to master networking in-depth to improve the effectiveness of intrusion detection training.

Assessment: GIAC Certified Intrusion Analyst (GCIA) Examination

ACS 4542: Web App Pen Testing and Ethical Hacking (3 credits)

With in-depth, hands-on labs and high-quality course content, AC4542 helps students move beyond push-button scanning to professional, thorough, and high-value web application testing. This enables students to demonstrate the impact of inadequate security that plagues most organizations' websites. Students will learn to apply a detailed, four-step methodology to web application penetration tests (reconnaissance, mapping, discovery, and exploitation); analyze the results from automated web testing tools to validate findings, determine their business impact, and eliminate false positives; manually discover key web application flaws; use Python to create testing and exploitation scripts during a penetration test; discover and exploit SQL Injection flaws to determine true risk to the victim organization; create configurations and test payloads within other web attacks; fuzz potential inputs for injection attacks; explain the impact of exploitation of web application flaws; analyze traffic between the client and the server application using tools such as the Zed Attack Proxy and Burp Suite to find security issues within the client-side application code; manually discover and exploit Cross-Site Request Forgery attacks; use the Browser Exploitation Framework to hook victim browsers; attack client software and the network, and evaluate the potential impact that XSS flaws have within an application; and perform a complete web penetration test during the Capture the Flag exercise to bring techniques and tools together into a comprehensive test. ACS 4542 is an expansion of SANS Course SEC542, with the addition of a series of enrichment exercises that strengthen students' ability to work in Python and understand how the networks and operating systems enable web attacks to succeed so as to become even more insightful penetration testers.

Assessment: Certified Web Application Penetration Tester (GWAPT) examination

ACS 4560: Network Penetration Testing and Ethical Hacking (3 credits)

This course teaches students how to test their own systems before malicious actors attack and how to become independent pen testers with far greater skill and knowledge than they would learn from traditional ethical hacking courses. Students will learn to develop tailored scoping and rules of engagement for penetration testing projects to ensure that the work is focused, well defined, and conducted in a safe manner; conduct detailed reconnaissance using document metadata, search engines, and other publicly available information sources to build a technical and organizational understanding of the target environment; use the Nmap scanning tool to conduct comprehensive network sweeps, port scans, Operating System fingerprinting, and version scanning to develop a map of target environments; choose and properly execute Nmap Scripting Engine scripts to extract detailed information from target systems; configure and launch the Nessus vulnerability scanner so that it discovers vulnerabilities through both authenticated and unauthenticated scans in a safe manner, and customize the output from such tools to represent the business risk to the organization; analyze the output of scanning tools to manually verify findings and perform false positive reduction using Netcat and the Scapy packet crafting tools; utilize the Windows and Linux command lines to plunder target systems for vital information that can further overall penetration test progress; establish pivots for deeper compromise and help determine business risks; configure the Metasploit exploitation tool to scan, exploit, and then pivot through a target environment in-depth; conduct comprehensive password attacks against an environment, including automated password guessing (while avoiding account lockout), traditional password cracking, rainbow table password cracking, and pass-the-hash attacks; utilize wireless attack tools for Wifi networks to discover access points and clients (actively and passively); crack WEP/WPA/WPA2 keys and exploit client machines included within a project's scope; and launch web application vulnerability scanners such as ZAP and then manually exploit Cross-Site Request Forgery, Cross-Site Scripting, Command Injection, and SQL injection attacks to determine the business risks faced by an organization. ACS 4560 is an expanded version of SANS Course SEC560, adding extensive networking and operating system and hardware and exploit exercises.

Assessment: Certified Penetration Tester (GPEN) examination

2. Educational Objectives and Intended Student Learning Outcomes

The two primary educational objectives of the program are to:

a) Produce candidates for the many critically important but currently open and unfilled jobs for skilled cybersecurity professionals at mid-size and large commercial or government enterprises in Maryland and other states; and
b) Create an accelerated path for a large number of associate's degree or higher degree holders who demonstrate a high level of aptitude for cybersecurity-related work to enter the workforce with a credible and applicable set of skills that are attractive to employers, enabling graduates to attain jobs with above-average compensation and attractive career prospects.

The intended student learning outcomes are directly related to the fulfillment of these objectives:

- Students will be able to utilize a broad range of current tools and technologies in the design and implementation of defensive security solutions that may be deployed across an organization's computing and network environment.
- Students will be able to assemble tools and configure systems and networks to permit systems to foster resiliency and continuity of operations through attacks.
- Students will be able to understand the most prevalent methods and vectors used in cyber-attacks in order to assess the vulnerabilities of an organization relative to these attack vectors, and to respond to incidents associated with these activities within their organization.
- Students will build upon these baseline skills and choose to begin to specialize in a particular area of information security practice associated with a more specialized and job-specific role, including advanced defensive techniques, vulnerability analysis and penetration testing, or digital forensics.

Each learning outcome of the CACS program 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.

The latest versions of these learning objectives, measured by each of the relevant GIAC exams, may be found at the following links for the respective certifications:

Required Courses:

1. For ACS 2201: Technology Essentials learning objectives are to demonstrate the ability to use each of the technology elements listed in the course syllabus.

2. For ACS 3401: GIAC Security Essentials Certification Exam (GSEC)
https://www.giac.org/certification/security-essentials-gsec

3. For ACS 3504: GIAC Security Incident Handling and Hacker Exploits Certification Exam (GCIH)

https://www.giac.org/certification/certified-incident-handler-gcih

Elective Choices:

- For ACS 4508: Certified Forensic Examiner Exam (GCFE) https://www.giac.org/certification/certified-forensic-examiner-gcfe

- For ACS 4410: Certified Industrial Cybersecurity Professional Exam (GICSP) https://www.giac.org/certification/global-industrial-cyber-security-professional-gicsp

- For ACS 4501: Certified Enterprise Defender Exam (GCED) https://www.giac.org/certification/certified-enterprise-defender-gced

- For ACS 4503: Certified Intrusion Analyst Exam (GCIA) https://www.giac.org/certification/certified-intrusion-analyst-gcia

- For ACS 4542: Certified Web Application Penetration Tester Exam (GWAPTT) https://www.giac.org/certification/web-application-penetration-tester-GWAPTt

- For ACS 4560: Certified Penetration Tester Exam (GPEN) https://www.giac.org/certification/penetration-tester-gpen

Certification exams used by the CACS program are in turn certified by the American National Standards Institute. 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. Because no students will be awarded a CACS degree if they fail to pass any of the GIAC exams required by the program, student success on the GIAC exams correlates to achievement of the learning outcomes targeted by the CACS program.

3. How General Education Requirements Will Be Met

As an upper division certificate program, the CACS does not include general education requirements. However, some mastery of the eight knowledge and skill areas of the Maryland General Education requirements listed in COMAR 13B.06.01 are often as important as technical skills to the ultimate career success of cybersecurity professionals, especially with regard to their ability to lead others to higher performance. To ensure that our students have a solid foundation in meeting those requirements, STI has established a minimum of 24 credits of general education and a grade point average of 3.0 on those courses for acceptance into the CACS program.

4. Specialized Accreditation/Certification Requirements

Each student who earns a CACS certificate will have achieved certification in three areas of cybersecurity using Global Information Assurance Certifications (GIAC). The two broader GIAC certifications of CACS (GSEC and GCIH) are specified by the U.S. Department of Defense under DOD Directives 8570 and 8140 as proof that employees and contractors meet the requirements for employment in the highest levels (II and III, respectively) of Technical Information Assurance roles. The third CACS-required certification affirms graduates are prepared for specific – generally higher-paying – roles in cybersecurity.

5. Contract with Another Institution or Non-collegiate Organization

Under a formal Memorandum of Understanding (MOU), STI outsources to SANS (STI's parent organization) many of the operational and administrative functions required to support operations, including establishment of most of our learning environments (physical and virtual), financial transactions, accounting, technology, and other administrative support services. Using this mechanism, STI benefits from SANS's economies of scale and transforms typically high-fixed cost elements into manageable, smaller variable costs. STI also benefits from its relationship with Global Information Assurance Certification (GIAC), a sister company also owned by SANS. GIAC was established in 1999 to develop and offer exams and certifications that validate whether an individual has gained sufficient competency or mastery of the complex topics taught in SANS courses, and most technical STI courses require students to pass a GIAC certification exam. GIAC exams are the product of broad-based job task analyses that incorporate feedback from hundreds of industry participants. Exam questions and answers and scoring patterns are reviewed and assessed by a PhD in psychometrics. Many of these certification exams have been designed with such a degree of quality that they are, themselves, certified by the American National Standards Institute (ANSI). Thus, learning in STI's CACS courses is validated not by exams created by individual faculty members, but by assessments created by a highly specialized exam creation and testing organization that also keeps these exams current with changing professional requirements over time.

The MOUs have enabled all STI degree programs since STI was established and were most recently reviewed and approved during the Middle States accreditation team visit. A more complete description of the corporate entities, along with the MOUs, is provided in Appendix 2.

H. Adequacy of Articulation

As an upper division certificate program, STI's CACS program does not include credits for lower-level courses. Thus, no articulation agreements are anticipated. Admission to the CACS program requires completion of 24 credits of general education courses. STI will rely on continuing Middle States accreditation of each partner institution to ensure the adequacy of the general education requirements of each partner institution.

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

The faculty serving the students of the proposed CACS 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 five-year re-accreditation review. Adding 1,500 students to the instructors' teaching load is the equivalent of a 3% 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.

Examples of STI faculty members who are directly associated with the courses included in the CACS program are described below.

Ed Skoudis

Ed Skoudis has taught cyber incident response and advanced penetration testing techniques to more than 12,000 cybersecurity professionals. He is a SANS Faculty Fellow and the lead for the SANS Penetration Testing Curriculum. His courses distill the essence of real-world, front-line case studies he accumulates because he is consistently one of the first experts brought in to provide after-attack analysis on major breaches where credit card and other sensitive financial data are lost. Each year he keynotes the RSA conference, the largest conference in the field, along with SANS faculty members Johannes Ullrich and James Lyne. Their keynote presents the most dangerous new attacks these experts foresee becoming damaging in the coming year. Ed led the team that built NetWars, the low-cost, widely used cyber training and skills assessment ranges relied upon by military units and corporations with major assets at risk. His team also built CyberCity, the fully authentic urban cyber warfare simulator that was featured on the front page of the *Washington Post*. He was also the expert called in by the White House to test the security viability of the Trusted Internet Connection (TIC) that now protects U.S. government networks, and he led the team that first publicly demonstrated significant security flaws in virtual machine technology. He has the rare capability to translate advanced technical knowledge into easy-to-master guidance as demonstrated by the popularity of his step-by-step *Counter Hack* books. Ed earned an M.S. in information networking from Carnegie Mellon University, and a B.S. in electrical engineering from the University of Michigan, summa cum laude.

Ed created and teaches both ACS 4504: Incident Handling and Hacker Exploits and ACS 4560: Network Penetration Testing and Ethical Hacking.

Dr. Johannes Ullrich

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

Johannes teaches ACS 4503: Intrusion Detection In-Depth.

Dr. Eric Cole

Eric served as CTO of McAfee and Chief Scientist for Lockheed Martin, and is the author of several books, including *Advanced Persistent Threat, Hackers Beware, Hiding in Plain Sight, Network Security Bible 2nd Edition*, and *Insider Threat*. He is the inventor of over 20 patents and is a researcher, writer, and speaker. He was also a member of the Commission on Cyber Security for the 44th President and several executive advisory boards. Eric provides consulting services and expert witness work, and he leads research and development initiatives to advance the state-of-the-art in information systems security. He was the lone inductee into the InfoSec European Hall of Fame in 2014. Eric earned a doctorate from Pace University with a concentration in information security focused on steganography.

Eric teaches ACS 4401: Security Essentials.

Rob Lee

Rob is the curriculum lead and author for digital forensic and incident response training at the SANS Institute. Rob has more than 18 years of experience in digital forensics, vulnerability and exploit discovery, intrusion detection/prevention, and incident response. Rob graduated from the U.S. Air Force Academy and served as a founding member of the 609th Information Warfare Squadron, the first U.S. military operational unit focused on information operations. Later, he was a member of the Air Force Office of Special Investigations, where he led a team conducting computer crime investigations, incident response, and computer forensics. He worked with the U.S. Department of Defense and intelligence communities as the technical lead for a vulnerability discovery and an exploit development team, lead for a cyber forensics branch, and lead for a digital forensic and security software development team. Rob was also a director for Mandiant (currently the forensics arm of FireEye), a company focused on investigating advanced adversaries, such as the APT. He is a co-author of the Mandiant threat intelligence report *M-Trends: The Advanced Persistent Threat*. Rob also co-authored the book *Know Your Enemy*. He earned his MBA from Georgetown University.

Rob created and teaches ACS 4508: Advanced Digital Forensics and Incident Response

Michael Assante

Michael Assante is Director of Industrials and Infrastructure at the SANS Institute, an area focused on securing organizations that make, move, and power the world. He is also the SANS lead for Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) security. He served as Vice President and Chief Security Officer (CSO) at American Electric Power, undertook research on the vulnerability of electric generators to destruction through remote cyber-attack (for the Idaho National

Laboratory), and served as the first CSO at the North American Electric Reliability Corporation, which is responsible for managing the electric grid for North America. Government, intelligence, and military organizations have also relied on his leadership and counsel for more than 20 years. As a Senior Associate with the Center for Strategic and International Studies Strategic Technologies Program, Michael authors papers and provides views on policy issues. He has testified before the U.S. Senate and House and was an initial member of the Commission on Cyber Security for the 44th Presidency. He chairs the SANS ICS Security Summit, now in its 13th year, presenting co-authored reports such as *Outpacing Cyber Threats - Priorities for Cybersecurity at Nuclear Facilities* for the Nuclear Threat Institute. His work in ICS security has been widely recognized and he was selected by his peers as the winner of *Information Security Magazine's* Security Leadership Award for his efforts as a strategic thinker. The RSA 2005 Conference awarded him its Outstanding Achievement Award in the practice of security within an organization.

Mike created and teaches ACS 4410: ICS/SCADA Security Essentials

Stephen Sims
Stephen Sims is an industry expert with over 15 years of experience in information technology and security. Stephen currently works out of San Francisco as a consultant performing reverse engineering, exploit development, threat modeling, and penetration testing. He has a MS in information assurance from Norwich University and is a Faculty Fellow for the SANS Institute and author of SANS' only 700-level course, SEC760: Advanced Exploit Development for Penetration Testers, which concentrates on complex heap overflows, patch diffing, and client-side exploits. Stephen is also the lead author on SEC660: Advanced Penetration Testing, Exploits, and Ethical Hacking. He holds the GIAC Security Expert (GSE) certification as well as the CISSP®, CISA, Immunity NOP, and many other certifications.

Stephen teaches ACS 4501: Enterprise Defender.

Seth Misenar
Seth is a cybersecurity expert who serves as a Senior Instructor with the SANS Institute and Principal Consultant at Context Security, LLC. He is numbered among the few security experts worldwide to have achieved the GIAC GSE (#28) credential. Seth teaches several cybersecurity courses for the SANS Institute, including two very popular courses for which he is lead author: the bestselling SEC511: Continuous Monitoring and Security Operations, and SEC542: Web Application Penetration Testing and Ethical Hacking. Seth's background includes security research, network and web application penetration testing, intrusion analysis, incident response, and security architecture design. He previously served as a security consultant for Fortune 100 companies, as well as the HIPAA Security Officer for a state government agency. Seth also co-authored the *Syngress CISSP® Study Guide*, now in its third edition, and the *Eleventh Hour CISSP®: Study Guide*. He is the course author for MGT414: SANS Training Program for CISSP® Certification. Seth has a bachelor of science degree in philosophy from Millsaps College.

Seth co-created and teaches ACS 4542: Web App Pen Testing and Ethical Hacking.

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, whichcontains 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 CACS students each year with a cumulative capacity of more than 40,000 students. Each year the residential program expands by 10 to 20 institutes. Thus, the proposed program will easily be accommodated in the existing in-person training programs.

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

L. Adequacy of Financial Resources with Documentation (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					
2. Tuition/Fee Revenue (c + g below)	1,248,000	3,120,000	6,240,000	9,360,000	12,480,000
a. Number of F/T Students	40	100	200	300	400
b. Annual Tuition/Fee Rate	12,000	12,000	12,000	12,000	12,000
c. Total F/T Revenue (a x b)	480,000	1,200,000	2,400,000	3,600,000	4,800,000
d. Number of P/T Students	80	200	400	600	800
e. Credit Hour Rate	1,000	1,000	1,000	1,000	1,000
f. Annual Credit Hour Rate	12	12	12	12	12
g. Total P/T Revenue (d x e x f)	768,000	1,920,000	3,840,000	5,760,000	7,680,000
3. Grants, Contracts & Other External Sources	-	-	-	-	-
4. Other Sources	-	-	-	-	-
TOTAL (Add 1 – 4)	1,248,000	3,120,000	6,240,000	9,360,000	12,480,000

Table 2: EXPENDITURES					
Expenditure Categories	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**
1. Faculty (b + c below)	48,600	121,500	243,000	364,500	486,000
a. # Sections offered	2	5	10	15	20
b. Total Salary	36,450	91,125	182,250	273,375	364,500
c. Total Benefits	12,150	30,375	60,750	91,125	121,500
2. Admin. Staff (b + c below)	336,000	784,000	1,568,000	2,352,000	3,360,000
a. # FTE	3	7	14	21	30
b. Total Salary	240,000	560,000	1,120,000	1,680,000	2,400,000
c. Total Benefits	96,000	224,000	448,000	672,000	960,000
3. Support Staff (b + c below)	252,000	672,000	1,344,000	2,016,000	2,688,000
a. # FTE	3	8	16	24	32
b. Total Salary	180,000	480,000	960,000	1,440,000	1,920,000
c. Total Benefits	72,000	192,000	384,000	576,000	768,000
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	599,400	1,498,500	2,997,000	4,495,500	5,994,000
TOTAL (Add 1 – 7)	1,236,000	3,076,000	6,152,000	9,228,000	12,528,000

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.
   The tuition projection for Year 1 assumes the CACS program admits 40 full-time students who each pay $15,000 for a semester, plus another 80 students who complete the program part-time, also paying $15,000. We believe this is an appropriate estimate given that we have been able to attract that many students to immersion academies in Maryland without the benefit of the public relations and marketing work that will be associated with the launch of this program.

   The revenue projection is stated net of the assumption that 1 out of 5 students will be successful and that STI will need to reimburse them (or their loan provider) for their participation. This is in-line with the graduation and placement rates of past Cyber Immersion Academies.

   In each subsequent year, we project that enrollment will progress to 300, then 600, then 900, and finally to 1,200 students completing the CACS program in each of Years 2 – 5, with no planned tuition increases and no change in the percentage of admitted students who eventually are not responsible for the cost of the program. We believe expectations for significant growth are reasonable because we will be able to expand the offering of the program to students from other states, and because 1,200 students will still be less than 5% of the total number of professionals trained by STI's parent each year.

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
CACS 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. We estimate that this program will represent less than 4% of the total salary and benefits of the faculty involved, because this program is small relative to the total operations of SANS (more than 40,000 students in 2017). When they choose to take the course online, no additional faculty are required and, similarly in live classes, CACS students represent only a small fraction of those students being taught by the existing group of subject-matter experts and teaching assistants. Therefore, we do not anticipate any increase in the number of faculty required to teach CACS students, either live or online, beyond the natural growth of the SANS faculty.

While the costs associated with the faculty who teach these students is embedded in the payments associated with the Memorandum of Understanding between STI and SANS, we have separated out projected amounts for Faculty Salary and Faculty Benefits in Table 2.

Administrative and Support Staff
The STI graduate programs currently operate at a ratio of students to administrative staff ratio of 50:1 (including both full-time administrative and support staff). Because we anticipate the students in the CACS program will require more attention, particularly because of their job search and Title IV reimbursement activity, we projected expenses using a more conservative ratio of student to staff of 40:1 instead of 50:1. Average salary and benefit information is reflective of our current cost experience and market expectations.

Equipment, Library, New and/or Renovated Space
The CACS 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 CACS 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 CACS 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.

This three-level closed-loop assessment system has led to the extraordinary success of STI graduates and its substantial impact on major organizations, as documented in Appendix 3.

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).

As a key element of the rollout of this program, STI – working jointly with one of largest employer partners for SANS programs, Sandia National Labs – will invite Bowie State University to be the first collegiate partner for our program. Through a program already in place between Sandia and Bowie State University, we will enable all students at Bowie State to test their aptitude for and interest in cybersecurity. We will provide special coaching for students who show strong aptitude and provide them with enrichment programs in cybersecurity topics while they continue to study at Bowie State. Students who use the enrichment material and qualify for the CACS will be accepted into the CACS certificate program. As this program matures, we will widely disseminate information about how the program works to minority students to encourage more participation.

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 4 for the evidence that this program complies with the Principles of Good Practice.

Appendix 1. Letters from Employers Ready to Interview and Hire Students Who Master the Courses and Certifications of the CACS Program

DEFENSE POINT
SECURITY
An Accenture Federal Services Company

LETTER OF COMMITMENT

DEFENSE POINT SECURITY, LLC
44 CANAL CENTER PLAZA, SUITE 305
ALEXANDRIA, VA 22314

Dear SANS Institute:

The intent of this Letter is to provide a written expression of commitment of Defense Point Security, LLC to be an employer partner of the SANS Institute's Strategic Industry Partnership (SIP) in pursuit of the EARN Maryland (MD) Cybersecurity and Information Technology Industries grant solicitation issued on June 29, 2017. As an employer partner of this EARN MD SIP, Defense Point Security, LLC commits to consider hiring the graduates of the SANS Institute's proposed CyberTalent Immersion Academy training program ("Academy"). The provisions in this Letter of Commitment are nonbinding. This Letter does not guarantee that Employer will execute any hires of Academy graduates. Defense Point Security, LLC hires approximately 54 cybersecurity professionals each year, and based on the training and certifications to be earned in the Academy, believes the program would produce skilled graduates of hiring interest.

The individual signing this letter affirms they are an authorized representative of their respective organization and have authority to enter into this Letter of Commitment. Nothing herein shall be construed as an obligation to enter into a formal contract. It is subject to a withdrawal and modification at any time without occurring any legal liability or obligation.

Sincerely,

Dave Poole, Chief Operating Officer
Defense Point Security, LLC

DocuSigned by:
DBFC25B0B89E4E6...
________________________________ Date: 8/24/2017

GEICO

LETTER OF COMMITMENT

GEICO
1 GEICO Plaza
Washington DC. 20076

Dear SANS Institute:

The intent of this Letter is to provide a written expression of commitment of GEICO to be an employer partner of the SANS Institute's Strategic Industry Partnership (SIP) in pursuit of the EARN Maryland (MD) Cybersecurity and Information Technology Industries grant solicitation issued on June 29, 2017. GEICO's sole obligation on as an employer partner of this EARN MD SIP, means that GEICO commits to consider hiring the graduates of the SANS Institute's proposed CyberTalent Immersion Academy training program ("Academy") who apply for employment with GEICO. All provisions in this Letter of Commitment are nonbinding. This Letter does not guarantee that Employer will execute any hires of Academy graduates.

The SANS Institute understands that they may not issue any press releases or use GEICO's trademarks for any advertising, marketing or promotional purposes, or in any form on the Internet, without the express prior written consent of GEICO. Use of the "GEICO" name in mass release emails is strictly prohibited. Except as set forth in this paragraph, the SANS Institute shall not, under any circumstances, use, display, publish or distribute GEICO's name or trademarks, without the express written permission of GEICO.

The individual signing this letter affirms they are an authorized representative of their respective organization and have authority to enter into this Letter of Commitment. Nothing herein shall be construed as an obligation to enter into a formal contract. It is subject to a withdrawal and modification at any time without occurring any legal liability or obligation.

Sincerely,

John OKeefe, CISO & Infrastructure AVP
GEICO

DocuSigned by:
JOHN OKEEFE
FE11A67E684B4F1...
_______________________________ Date: September 12, 2017

CACI
EVER VIGILANT

LETTER OF COMMITMENT

CACI NSS, Inc.
11955 Freedom Drive
Reston, VA 20190

Dear SANS Institute:

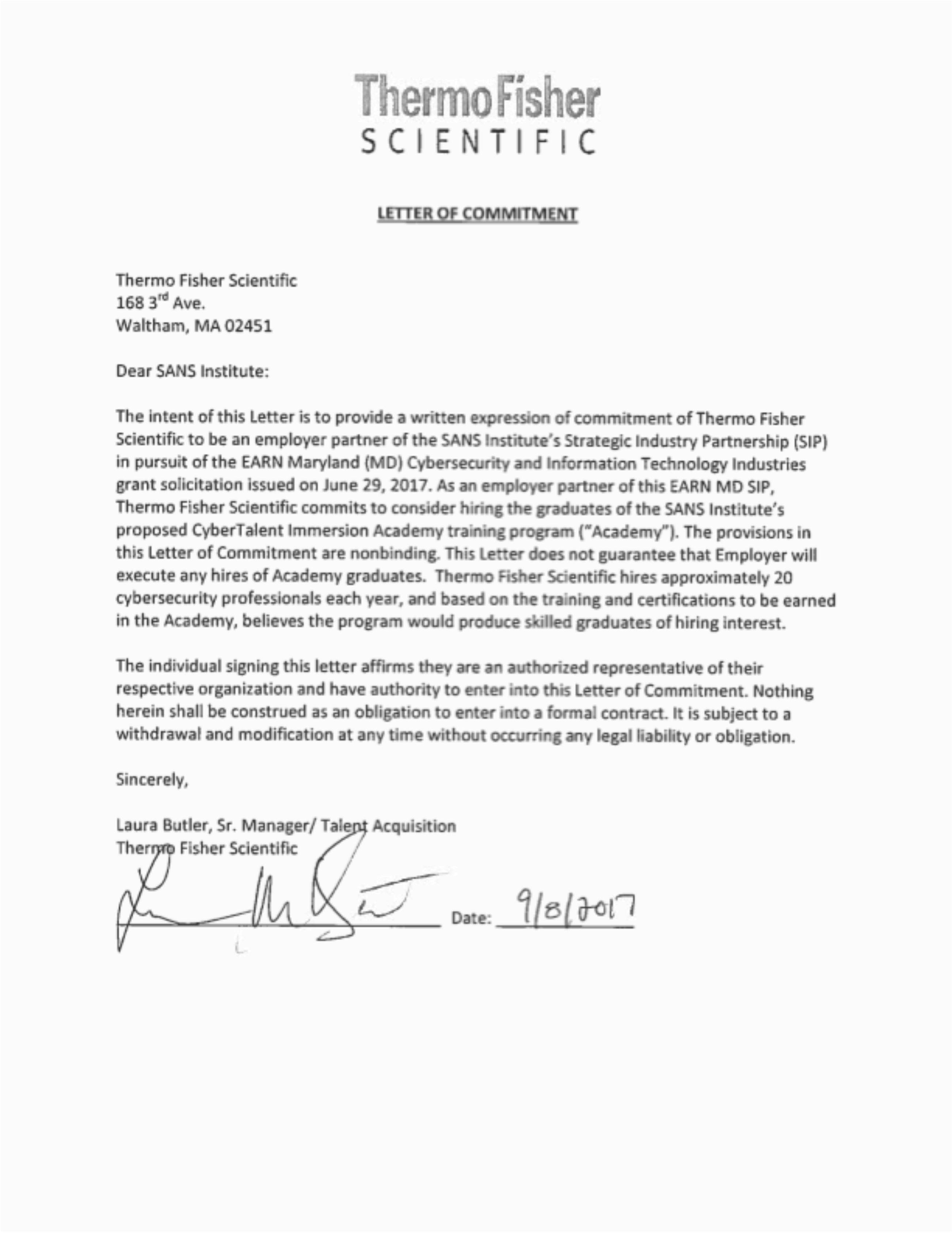
The intent of this Letter is to provide a written expression of commitment of CACI NSS, Inc. (CACI) to be an employer partner of the SANS Institute's Strategic Industry Partnership (SIP) in pursuit of the EARN Maryland (MD) Cybersecurity and Information Technology Industries grant solicitation issued on June 29, 2017. As an employer partner of this EARN MD SIP, CACI commits to consider hiring the graduates of the SANS Institute's proposed CyberTalent Immersion Academy training program ("Academy"). The provisions in this Letter of Commitment are nonbinding. This Letter does not guarantee that Employer will execute any hires of Academy graduates. CACI hires approximately 75-125 cybersecurity professionals each year, and based on the training and certifications to be earned in the Academy, believes the program would produce skilled graduates of hiring interest.

The individual signing this letter affirms they are an authorized representative of their respective organization and have authority to enter into this Letter of Commitment. Nothing herein shall be construed as an obligation to enter into a formal contract. It is subject to a withdrawal and modification at any time without occurring any legal liability or obligation.

Sincerely,

Calvin Freeman
Executive Director, Procurement
CACI NSS, Inc.

Date: 9/8/2017



ThermoFisher
SCIENTIFIC

LETTER OF COMMITMENT

Thermo Fisher Scientific
168 3rd Ave.
Waltham, MA 02451

Dear SANS Institute:

The intent of this Letter is to provide a written expression of commitment of Thermo Fisher Scientific to be an employer partner of the SANS Institute's Strategic Industry Partnership (SIP) in pursuit of the EARN Maryland (MD) Cybersecurity and Information Technology Industries grant solicitation issued on June 29, 2017. As an employer partner of this EARN MD SIP, Thermo Fisher Scientific commits to consider hiring the graduates of the SANS Institute's proposed CyberTalent Immersion Academy training program ("Academy"). The provisions in this Letter of Commitment are nonbinding. This Letter does not guarantee that Employer will execute any hires of Academy graduates. Thermo Fisher Scientific hires approximately 20 cybersecurity professionals each year, and based on the training and certifications to be earned in the Academy, believes the program would produce skilled graduates of hiring interest.

The individual signing this letter affirms they are an authorized representative of their respective organization and have authority to enter into this Letter of Commitment. Nothing herein shall be construed as an obligation to enter into a formal contract. It is subject to a withdrawal and modification at any time without occurring any legal liability or obligation.

Sincerely,

Laura Butler, Sr. Manager/ Talent Acquisition
Thermo Fisher Scientific

Date: 9/8/2017

Spry

LETTER OF COMMITMENT

Spry Methods
1420 Spring Hill Rd, Suite 300
McLean, VA 22102

Dear SANS Institute:

The intent of this Letter is to provide a written expression of commitment of Spry Methods to be an employer partner of the SANS Institute's Strategic Industry Partnership (SIP) for the EARN Maryland (MD) Cybersecurity and Information Technology Industries grant that will be implemented in 2018-2019. As an employer partner of this EARN MD SIP, Spry Methods commits to hiring consideration of the graduates of the SANS Cyber Workforce Academy ("Academy"). This Letter does not guarantee that Employer will execute any hires of Academy graduates. Spry Methods hires approximately 20 cybersecurity professionals each year, and based on the training and certifications to be earned in the Academy, believes the program would produce skilled graduates for hiring consideration.

The individual signing this letter affirms they are an authorized representative of their respective organization and have authority to enter into this Letter of Commitment. The provisions in this Letter of Commitment are nonbinding. Nothing herein shall be construed as an obligation to enter into a formal contract. It is subject to a withdrawal and modification at any time without occurring any legal liability or obligation.

Sincerely,

Jason Gebert, Program Manager
Spry Methods

_________________________________ Date: 2/2/2018

AERSTONE

Quest Consultants LLC
DBA Aerstone
12250 Rockville Pike
Suite 250
Rockville MD 20852

LETTER OF COMMITMENT

Dear SANS Institute:

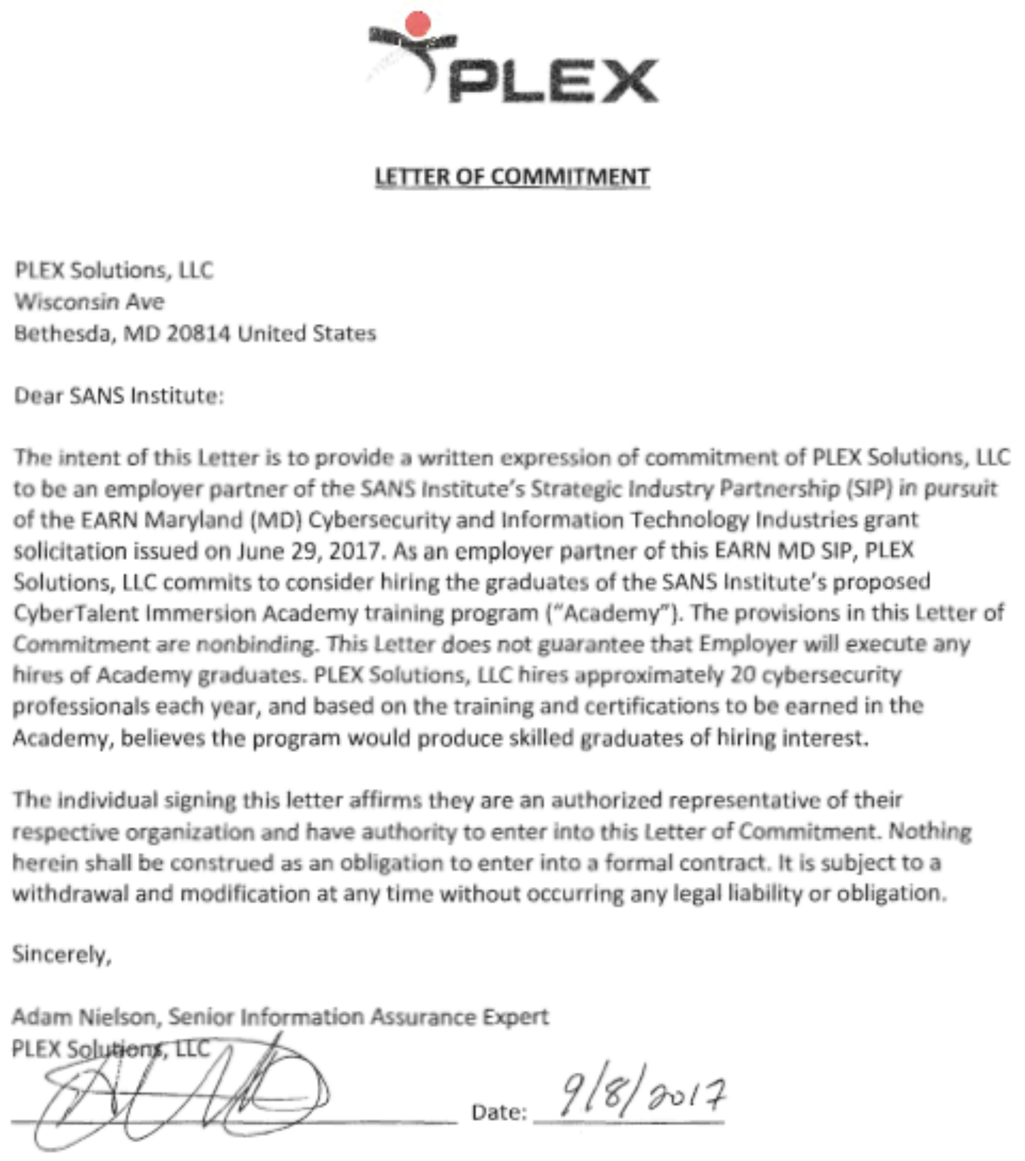
The intent of this Letter is to provide a written expression of commitment of Aerstone to be an employer partner of the SANS Institute’s Strategic Industry Partnership (SIP) for the EARN Maryland (MD) Cybersecurity and Information Technology Industries grant that will be implemented in 2018-2019. As an employer partner of this EARN MD SIP, Aerstone commits to hiring consideration of the graduates of the SANS Cyber Workforce Academy (“Academy”). This Letter does not guarantee that Employer will execute any hires of Academy graduates. Aerstone hires approximately 4 cybersecurity professionals each year, and based on the training and certifications to be earned in the Academy, believes the program would produce skilled graduates for hiring consideration.

The individual signing this letter affirms they are an authorized representative of their respective organization and have authority to enter into this Letter of Commitment. The provisions in this Letter of Commitment are nonbinding. Nothing herein shall be construed as an obligation to enter into a formal contract. It is subject to a withdrawal and modification at any time without occurring any legal liability or obligation.

Sincerely,

Francis W Schugar
Quest Consultants LLC DBA Aerstone

Francis W Schugar ______________ Date: 01/30/2018



PLEX

LETTER OF COMMITMENT

PLEX Solutions, LLC
Wisconsin Ave
Bethesda, MD 20814 United States

Dear SANS Institute:

The intent of this Letter is to provide a written expression of commitment of PLEX Solutions, LLC to be an employer partner of the SANS Institute's Strategic Industry Partnership (SIP) in pursuit of the EARN Maryland (MD) Cybersecurity and Information Technology Industries grant solicitation issued on June 29, 2017. As an employer partner of this EARN MD SIP, PLEX Solutions, LLC commits to consider hiring the graduates of the SANS Institute's proposed CyberTalent Immersion Academy training program ("Academy"). The provisions in this Letter of Commitment are nonbinding. This Letter does not guarantee that Employer will execute any hires of Academy graduates. PLEX Solutions, LLC hires approximately 20 cybersecurity professionals each year, and based on the training and certifications to be earned in the Academy, believes the program would produce skilled graduates of hiring interest.

The individual signing this letter affirms they are an authorized representative of their respective organization and have authority to enter into this Letter of Commitment. Nothing herein shall be construed as an obligation to enter into a formal contract. It is subject to a withdrawal and modification at any time without occurring any legal liability or obligation.

Sincerely,

Adam Nielson, Senior Information Assurance Expert
PLEX Solutions, LLC
_____________________________ Date: 9/8/2017

RBR-Technologies

LETTER OF COMMITMENT

RBR-Technologies, Inc.
2288 Blue Water Blvd
Suite 322
Odenton, MD 21113

Dear SANS Institute:

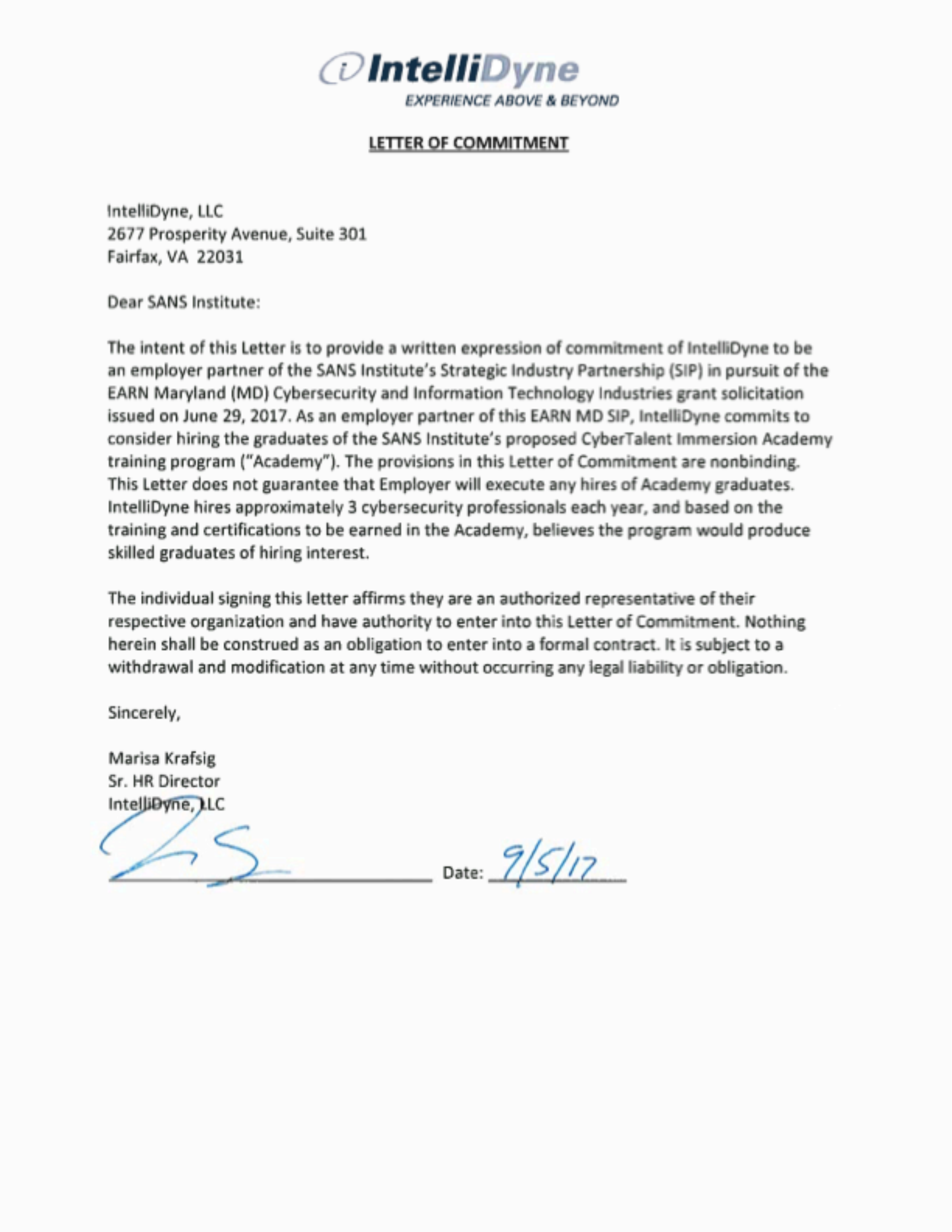
The intent of this Letter is to provide a written expression of commitment of RBR-Technologies, Inc. to be an employer partner of the SANS Institute's Strategic Industry Partnership (SIP) in pursuit of the EARN Maryland (MD) Cybersecurity and Information Technology Industries grant solicitation issued on June 29, 2017. As an employer partner of this EARN MD SIP, RBR-Technologies, Inc. commits to consider hiring the graduates of the SANS Institute's proposed CyberTalent Immersion Academy training program ("Academy"). The provisions in this Letter of Commitment are nonbinding. This Letter does not guarantee that Employer will execute any hires of Academy graduates. RBR-Technologies, Inc. hires approximately 5 cybersecurity professionals each year, and based on the training and certifications to be earned in the Academy, believes the program would produce skilled graduates of hiring interest. The cybersecurity roles RBR-Technologies, Inc. focus on include Information Systems Security Engineers, Security Intel Analysts, Cyber Network Defense Operators, which all require extensive training in order to possess the appropriate skill sets to be successful.

The individual signing this letter affirms they are an authorized representative of their respective organization and have authority to enter into this Letter of Commitment. Nothing herein shall be construed as an obligation to enter into a formal contract. It is subject to a withdrawal and modification at any time without occurring any legal liability or obligation.

Sincerely,

Jeff Rathmann, Chief Technology Officer
RBR-Technologies, Inc.

Jeff R________________________________ Date: _______________



IntelliDyne
EXPERIENCE ABOVE & BEYOND

LETTER OF COMMITMENT

IntelliDyne, LLC
2677 Prosperity Avenue, Suite 301
Fairfax, VA 22031

Dear SANS Institute:

The intent of this Letter is to provide a written expression of commitment of IntelliDyne to be an employer partner of the SANS Institute's Strategic Industry Partnership (SIP) in pursuit of the EARN Maryland (MD) Cybersecurity and Information Technology Industries grant solicitation issued on June 29, 2017. As an employer partner of this EARN MD SIP, IntelliDyne commits to consider hiring the graduates of the SANS Institute's proposed CyberTalent Immersion Academy training program ("Academy"). The provisions in this Letter of Commitment are nonbinding. This Letter does not guarantee that Employer will execute any hires of Academy graduates. IntelliDyne hires approximately 3 cybersecurity professionals each year, and based on the training and certifications to be earned in the Academy, believes the program would produce skilled graduates of hiring interest.

The individual signing this letter affirms they are an authorized representative of their respective organization and have authority to enter into this Letter of Commitment. Nothing herein shall be construed as an obligation to enter into a formal contract. It is subject to a withdrawal and modification at any time without occurring any legal liability or obligation.

Sincerely,

Marisa Krafsig
Sr. HR Director
IntelliDyne, LLC

_____________________ Date: 9/5/17

HALFAKER

CONTINUING TO SERVE

LETTER OF COMMITMENT

Halfaker & Associates, LLC
2900 S Quincy St #410
Arlington, VA 22206

Dear SANS Institute:

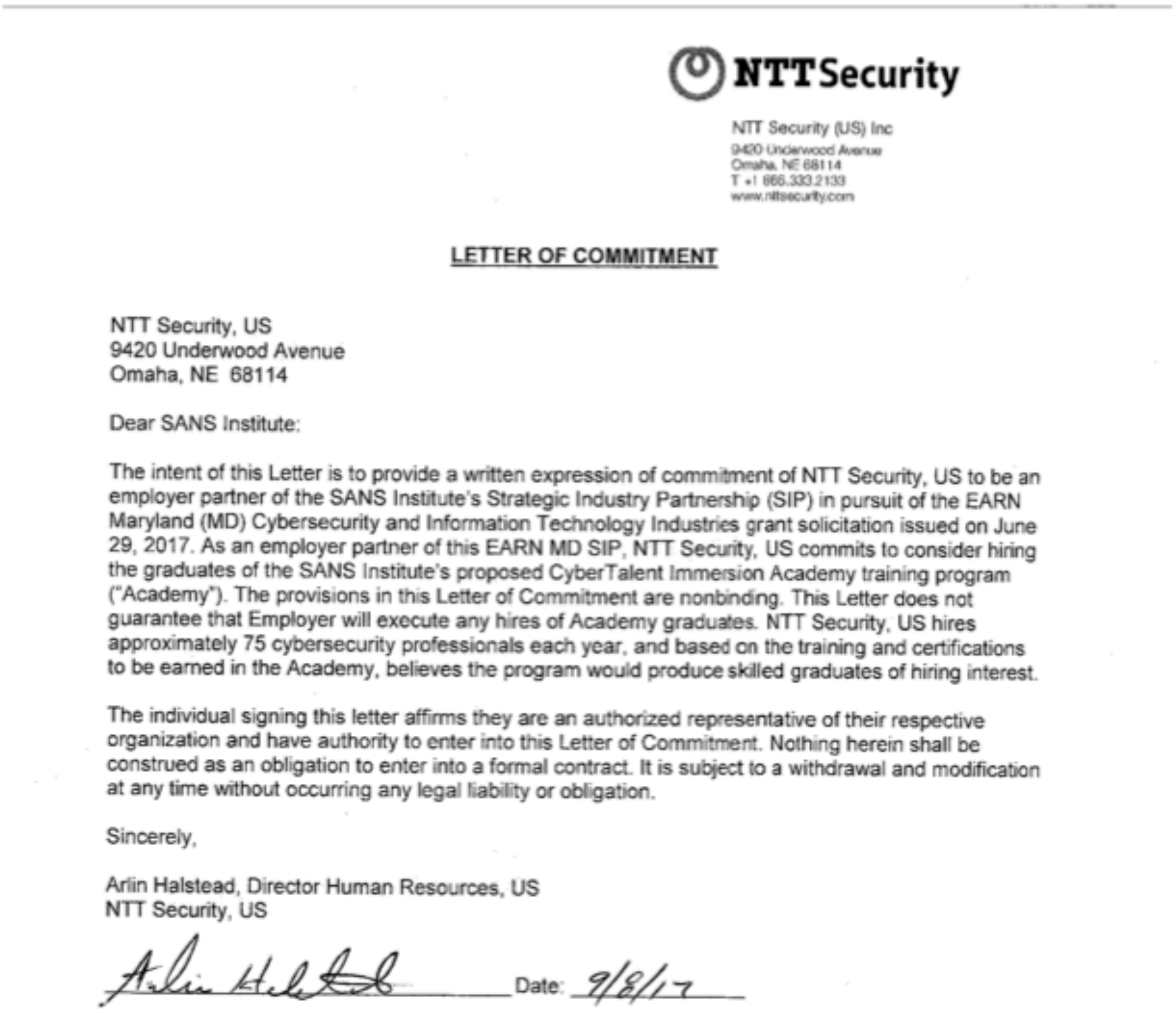
The intent of this Letter is to provide a written expression of commitment of Halfaker & Associates, LLC to be an employer partner of the SANS Institute’s Strategic Industry Partnership (SIP) for the EARN Maryland (MD) Cybersecurity and Information Technology Industries grant being implemented in 2018-2019. As an employer partner of this EARN MD SIP, Halfaker & Associates, LLC commits to hiring consideration of the graduates of the SANS Cyber Workforce Academy -Maryland (“Academy”). This Letter does not guarantee that Employer will execute any hires of Academy graduates. Halfaker & Associates, LLC hires approximately 10-12 cybersecurity professionals each year and based on the training and certifications to be earned by graduates in the Academy, believes the program would produce skilled candidates for hiring consideration.

The individual signing this letter affirms they are an authorized representative of their respective organization and have authority to enter into this Letter of Commitment. The provisions in this Letter of Commitment are nonbinding. Nothing herein shall be construed as an obligation to enter into a formal contract. It is subject to a withdrawal and modification at any time without occurring any legal liability or obligation.

Sincerely,

Jody Naleppa, Executive Vice President
Halfaker & Associates, LLC

Jody Naleppa Date: 03/16/18



NTTSecurity

NTT Security (US) Inc
9420 Underwood Avenue
Omaha, NE 68114
T +1 866.333.2133
www.nttsecurity.com

LETTER OF COMMITMENT

NTT Security, US
9420 Underwood Avenue
Omaha, NE 68114

Dear SANS Institute:

The intent of this Letter is to provide a written expression of commitment of NTT Security, US to be an employer partner of the SANS Institute's Strategic Industry Partnership (SIP) in pursuit of the EARN Maryland (MD) Cybersecurity and Information Technology Industries grant solicitation issued on June 29, 2017. As an employer partner of this EARN MD SIP, NTT Security, US commits to consider hiring the graduates of the SANS Institute's proposed CyberTalent Immersion Academy training program ("Academy"). The provisions in this Letter of Commitment are nonbinding. This Letter does not guarantee that Employer will execute any hires of Academy graduates. NTT Security, US hires approximately 75 cybersecurity professionals each year, and based on the training and certifications to be earned in the Academy, believes the program would produce skilled graduates of hiring interest.

The individual signing this letter affirms they are an authorized representative of their respective organization and have authority to enter into this Letter of Commitment. Nothing herein shall be construed as an obligation to enter into a formal contract. It is subject to a withdrawal and modification at any time without occurring any legal liability or obligation.

Sincerely,

Arlin Halstead, Director Human Resources, US
NTT Security, US

Arlin Halstead Date: 9/8/17

Appendix 2. Contracts with Related Entities

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

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

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

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

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

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

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

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

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

Purpose

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

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

Vision

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

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

Mission

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

Scope

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

Hours of Operations

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

Service Expectations

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

Accounting and Finance

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

Bursar & Registration

Process	Service Expectation	Service Metric

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

Human Resources

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

Marketing

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

Information Technology

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

Technical Course Maintenance & Presentation

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

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

Educational Residency

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

Service Constraints

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

Terms of Agreement

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

Periodic Quality Reviews

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

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

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

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

Service Level Maintenance

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

Issue Resolution

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

Payment Terms and Conditions

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

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

Agreed to on behalf of STI:	Agreed to on behalf of SANS:
____________________________	____________________________
Eric A. Patterson Executive Director SANS Technology Institute	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.

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

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 3. How Eight Extraordinary Cybersecurity Leaders Developed Their Management Capabilities

Summary: This annex shows how eight people made the transition from technologist to technology leader. Their experiences constitute a model for how to rapidly develop a much larger group of technical managers capable of leading teams of cybersecurity experts, and to ensure that those teams are doing the right things and that their work is of high quality and communicated effectively.

Contact Information: Alan Paller, President, The SANS Technology Institute, apaller@sans.edu

Background: The Challenge of Managing Technical Cybersecurity Teams

With tens of thousands of new cybersecurity professionals joining the work force, a new generation of managers is needed. They must be able to command the technical respect of the technologists, make wise decisions on optimal allocation of people and money, build bridges to other teams, and persuade other executives that cybersecurity initiatives and budgets are justified and cost-effective. Of these requirements, the most challenging to find among potential managers is the technical expertise to command the respect of people with advanced technical skills and to determine, with technical fidelity, what actually needs to be done to protect the specific systems for which they are responsible.

Because general managers rarely have technical skills, the direct path to leadership development in cybersecurity is the enhancement of management and communications skills for people with deep technical skills. An alternative path is simultaneous development of both deep technical skills and management skills. STI's graduate programs have been developing highly skilled technical cybersecurity managers for five years. The testimonials below offer a view of that program as seen through the eyes of extraordinary technical cybersecurity managers whom it has produced, as well as from the vantage point of a Citi leader who has sent many developing managers through the program.

Extraordinary Technical Cybersecurity Leaders

David Martin, Supervisory Special Agent, FBI Cyber Division, Technical Operations Unit

From inexperienced new FBI agent to supervisor of an elite FBI technical unit.

David Martin has worked in local, state, and federal law enforcement for the past 15 years. He has a Bachelor of Science in Computer Science from the University of Denver. When he began the STI Master of Science in Information Security Engineering (MSISE) program, he was an FBI agent investigating computer intrusion cases in the Detroit Field Office. As he developed additional technical and management skills through the program, he was promoted to Supervisory Special Agent in the Cyber Division's elite Technical Operations Unit. There, he is responsible for running CAT, the FBI's computer intrusion response "fly team," responding to the significant cyber threats facing our nation.

In David's own words: "The technical and leadership skills I learned at STI allowed me to progress from an inexperienced new agent to a forensics and incident response subject-matter expert, and also to become a supervisor of the most elite technical unit in the FBI."

Effective written and oral communication skills are keys to management success, and David has used those skills acquired through the MSISE to give back to the field. During his MSISE studies, David worked with his program advisors to publish and present research including *Tracing the Lineage of*

DarkSeoul, a case study of the April 2013 cyber-attack in South Korea, and *OS X as a Forensic Platform*, which examined the process of configuring a native OS X forensic environment that includes many open-source forensic tools. This latter paper served as a guide for David's own incident response team, and has proven to be useful to many other forensic professionals.

Michael C. Long II, Cyber Operations Specialist, U.S. Army Cyber Command

From a basic cybersecurity role to a "special mission unit" to a candidate for promotion.

Michael's last annual performance review specifically recognized his accomplishments in the STI MSISE program, including writing white papers, presenting his research at a national cybersecurity conference, winning Capture the Flag competitions, and earning industry-recognized skill-specific security certifications. Michael is currently waiting for the results of a centralized promotion board decision expected this fall.

The "cyber selection process" through which Michael won his assignment to serve on a special unit mission included over 50 hours of highly technical challenges, in-depth interviews, two papers, and more. Michael was one of six candidates selected from an initial pool of over 200 individuals. He attributes his success directly to the knowledge and skills gained through STI.

In Michael's own words: "As a result of the selection, I have been able to serve on many high-profile cyber operations, improving the security of systems across the Army. The skills I've learned in the MSISE program allowed me to take a leadership role in these operations, and I've been credited as being amongst the best Cyber Soldiers the Army has to offer. This work is challenging and rewarding, and I am grateful for the opportunity to serve, and for STI for helping me get here. STI allowed me to learn from the industry's best, and I am exceptionally grateful to have received the opportunity."

Jim Beechey, Director, Information Security, Consumers Energy

From being the sole InfoSec person to leading a team of 35 security professionals.

Just after he joined the MSISE program, Jim was hired by Consumers Energy as IT Security Manager. The CIO at Consumers credited his acceptance into STI as a key reason for offering him the leadership job.

In Jim's own words: "When I began the MSISE, I was leading a three-person team and was the lone InfoSec-focused person." By the end of the program in 2013, Jim explained, "my team is 35 strong and growing."

After earning his degree, Jim was promoted to Director, Information Security and has served in that role since.

Rod Currie, Information Systems Security Manager, The Boeing Company

From officer to lead to manager.

When Rod enrolled in STI in 2015, he was working as an Information Systems Security Officer at the Boeing Company. During the program, Rod was promoted to Program Security Lead, and was recently promoted again to Information Systems Security Manager.

Just before Rod began the MSISE in early 2015, he had been given a new title and a host of new leadership responsibilities, all unexpected and somewhat intimidating at the time. He was able to immediately apply what he learned in his STI courses to carry himself with confidence in his new role. Rod was recently promoted again, from Information Systems Security Officer (ISSO) to Information Systems Security Manager (ISSM), taking on responsibility and signature authority for all mission computer systems across several different flight-test locations.

Leadership within his organization has acknowledged Rod's development into a more competent, composed, and well-prepared incident handler as a result of the coursework at STI. Rod particularly valued learning how to build a risk prioritization matrix to present to management in the face of a staffing shortage and overall lack of support from leadership. The ability to effectively present risks to management and appeal to the individual stakeholders allowed him to drive the results he intended.

In terms of giving back to the field through his MSISE learning, Rod has done extensive research into automotive security. His published research includes *The Automotive Top 5: Applying the Critical Controls to the Modern Automobile* and *Hacking the CAN Bus: Basic Manipulation of a Modern Automobile Through CAN Bus Reverse Engineering*.

John Hally, Technical Director of Information Security, EBSCO

Returning to take a senior security position supported by confidence gained at STI.

When John enrolled at STI in 2007, he was working as a network and information security engineering team lead at EBSCO. Shortly after graduating from STI, John left EBSCO to pursue some independent opportunities, returning to EBSCO in 2015 in a senior security position.

John notes that the MSISE enabled him to bridge the gap between the technical aspects of his work and the equally important project and business processes that are part of his portfolio in his more senior current role. His ability to merge the technical and leadership components of information security "is a direct result of the broad range of skills and competencies that I have learned during my STI studies," John explained.

In John's own words: "What would I tell a CISO about supporting an employee in the program? I'd tell him that he's going to get his employee the very best hands-on technical education, sure. But it goes well beyond that. The STI master's program opens extraordinary access to a knowledge base when you need it. Not just the faculty that I got to know, but my peers as well. I can't tell you how many times I've bounced things off other graduates or students – it's one of those intangibles that people need to understand makes all the difference. You're in a program with people from every walk of life in security – financials, healthcare, oil & gas, three-letter agencies – clearly someone you know has hit or struggled with whatever you're going through, and you can reach out and ask."

Aron Warren, Technical Lead, Sandia National Laboratories

Moving up to technical lead before even graduating from STI.

When Aron enrolled at STI in 2011, he was a member of the technical staff at Sandia. Having set himself the goal of being promoted to technical lead, Aron landed the job before completing the program, which is not uncommon for STI master's degree students. "Every time I reflect on what has transpired during the work week it still excites me when I see how the MSISE taught the skills to be a better technical lead," Aron explained.

Reflecting on the topic of leadership in the field of information security from this new role and perspective, Aron says that "Organizations value those who can lead because so many can't. In this regard, the MSISE design is spot on. Courses are geared towards building both leadership capabilities and in-depth technical skills. The program, with its management courses, public speaking requirements, and realistic and challenging group projects was really beneficial in developing my leadership skills."

In terms of giving back through the MSISE: Aron's wide-ranging papers and presentations include:

1. *An In-depth Look at Tuckman's Ladder and Subsequent Works as a Tool for Managing a Project Team*
2. *Tor Browser Artifacts in Windows 10*
3. *Using Sulley to Protocol Fuzz for Linux Software Vulnerabilities*
4. *Setting up Splunk for Event Correlation in Your Home Lab*
5. *InfiniBand Fabric and Userland Attacks*
6. *Diskless Cluster Computing: Security Benefit of oneSIS and Git*

Michael Weeks, Security and Threat Intelligence Analyst in Critical Infrastructure in the electric sector and Cyber Operator for the U.S. Air Force Reserve

Military promotions and published research.

Michael's studies at STI took his technical, leadership, and managerial skills to the next level. Because of the knowledge he gained while in the program, he was promoted to Security Operations Center (SOC) Manager. Michael was also promoted within the U.S. Air Force Reserve to E-9 in a cybersecurity role.

Michael particularly valued learning Malware Analysis and Reverse-Engineering as part of the program, and his published research includes *Intrusion Analysis Using Windows PowerShell* and *Application White-listing with Bit9 Parity.*

Rich Arellano, Program Manager, Citi Security & Investigative Services, Citigroup

Citi executive sees STI graduates as setting the bar for its other employees.

As a leader at Citi, Rich has sent many developing managers through the MSISE program.

In Rich's own words: "A key goal of the Citi executives who decided to send employees to STI was to help our security professionals write better reports on key security issues. Security improvements become reality only if they are communicated effectively by leaders in the organization. We can now prove that the people who are participating in STI are contributing to the leadership effort by writing more effective security reports than the other people we have working on information security. One of our Citi group managers has said that his STI participants have 'set the bar for how to present security information effectively, and that the other people in the group now try to raise their game to meet that standard.' That is the leadership that we need, and we are getting it from our employees who are in enrolled at STI."

Additional Statements from Students and Alumni on the Effectiveness of STI

“I was able to immediately apply my newly acquired knowledge to solve emerging problems at work, earning a solid reputation as a trustworthy subject-matter expert in the process.” - Eric Jodoin, Cyber Operations Planner, Canadian Department of National Defense

“I have seen a direct correlation between my education and my professional career. From both public speaking to technical capabilities, I have increased my confidence and technical knowledge, allowing me to be a more productive member within my team.” - Nathaniel Quist, Incident Response Engineer, LogRhythm

“I looked at a number of different programs, and the decision-making process looked like this – I don’t need more theory, I need more practical, hands-on experience, and that’s exactly what STI offers.”
- Kevin Altman, Engineer-in-Charge/Program Manager, ICS Cyber Security, TransCanada

“The STI faculty make this program unique. They’re at the top of their industry and not a single one is too busy to engage with students at all levels.” - Ron Hamann, Security Analyst, Rackspace

“I wanted a degree that would empower me to leverage technology to create synergistic effects in the workplace in order to move my organization at the speed of success. In a time-critical engagement nothing pays dividends like practical experience. STI focuses on application of the latest cyber techniques in pursuit of objectives commonly encountered on the cyber operations floor.” - Matthew Toussain, U.S. Air Force)

“Hands down, SANS Technology Institute is one of the best organizations around and a thought leader in the cybersecurity community. It’s great to learn, to contribute and to be a part of an organization that is at the forefront of both academics and in the cybersecurity field.” - Joe Faust, Security Technical Operations Manager, Holy Redeemer Health System

“I’ve talked to a few friends who did information security master’s programs at traditional universities and all of them said it was more or less just to get the piece of paper. At least one of them is considering getting another master’s through SANS to try to build out more technical skills and get his name out there. You just don’t get that kind of return from most universities. Even parts of the MS program that didn’t feel good to me at the time, like getting lambasted by Stephen Northcutt on one of my papers, have helped me out far more than just checking off the block to get a degree.” - Stephen Deck, Senior Security Consultant, DirectDefense

“Ten years ago, almost to the day, I decided to change careers….I wanted to be in information security, it was an absolute....I have only been able to accomplish what’s come to fruition in no small part thanks to the people at STI. From the curriculum, the students, the instructors, the faculty... this institution has changed my life for the better, without question, in so many ways. This day, and every day hereafter, I am deeply proud to be a graduate of STI.” - Russ McRee, Principal Group Program Manager, Microsoft

A Final Word

In July 2017, STI awarded 28 masters degrees, a quadrupling of the number of degrees over the previous graduation. More than 150 technical cybersecurity professionals are now enrolled in the program, a doubling over just two years. We plan to expand the program to 1,000 students by 2021.

Appendix 4. Evidence of Compliance with the Principles of Good Practice (outlined in COMAR 13B02.03.22C)

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

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

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

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

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

(a) Curriculum and instruction

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

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

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

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

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

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

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

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

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

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

The learning outcomes of the courses included in the 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:

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

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

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

o 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.

o Return early after lunch to log back into GoToTraining

o Make sure your Internet connection is wired and not shared by the students.

o Make sure to have the vLive emergency contact info on hand.

o 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:

o Make sure that the OnSite students are aware of the virtual students.

o Be available for remote students before or after class in the Elluminate Office session.

o Depending on the class size and your teaching style you might need longer than usual to prepare for class (questions, demos, labs).

o 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. For example, for ACS 3504: Incident Handling and Hacker Exploits, the corresponding course site at SANS (https://www.sans.org/course/hacker-techniques-exploits-incident-handling) provides detailed technical requirements as well as a tech support contact to help students ensure they have the right equipment and software versions.

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

- The availability of academic support services and financial aid resources is posted at https://www.sans.edu/students/services, and on page 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.4.2. 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 CACS 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 CACS 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 CACS 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 CACS program

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

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

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

Ultimate student achievement in the CACS 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.4.3. 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 CACS program, by delivery modality.