Developing Leaders in Information Security

Earn Your Master’s Degree in Information Security.
Classes start April 15, 2011 in the Washington, DC area.
Application deadline is April 1, 2011.

STI Cohort 2013
Kevin Bong – Master of Science Degree in Information Security Engineering, SANS Technology Institute, 2009.
Kevin Bong graduated in 2009 and is the director of Security for Johnson Financial Group.

Eric Conrad – Master of Science Degree in Information Security Engineering, SANS Technology Institute, 2009
Eric Conrad graduated in 2009. He is a Certified SANS Instructor and the lead author of the book *The CISSP Study Guide* and is President of Backshore Communications, a company focusing on intrusion detection, incident handling, information warfare, and penetration testing.

Rick Smith – Master of Science Degree in Information Security Engineering, SANS Technology Institute, 2009
Rick Smith graduated in 2009 and is a Principal Cyber Security Engineer for Science Application International Corporation (SAIC) where he provides information security consulting services to Department of Defense, other federal civilian government agencies, and commercial organization.

Stephen Northcutt – President, SANS Technology Institute
Mission Statement

The mission of the SANS Technology Institute is to develop the information security technology leaders needed to help strengthen the information community all over the world by improving the security of cyberspace. SANS Technology Institute seeks to prepare both the managers of information security groups and the technical leaders who direct security technology programs. SANS Technology Institute’s primary functional emphasis is instruction, but the Institute’s faculty and students will engage in research and public service programs.

STI’s Catalog – www.sans.edu

This brochure contains general information about the SANS Technology Institute (STI) and the STI Cohort 2013 option. STI’s complete catalog is available online at www.sans.edu. Please visit the Web site for the latest information. Please note that the admission and curriculum requirements in effect when a person is admitted to STI are the requirements that will apply to that person.
A Letter from the President

The SANS Technology Institute (STI) offers students a unique opportunity to become leaders in the information security field. At STI, the wisdom of industry and business, college academia, and practical skills merge as students are taught by leaders with a demonstrated track record of leadership, knowledge, and expertise in information technology and security.

We are excited to announce the STI Cohort 2013. This accelerated option is designed for students who want to earn a Master of Science in Information Security Management (MSISM) or a Master of Science in Information Security Engineering (MSISE) degree in two years and share their learning experience with an exclusive group of students.

**The STI Cohort 2013 starts April 15, 2011 in the Washington, DC area and students will graduate in June of 2013.** Applications are currently being accepted and will close April 1, 2011. This brochure provides details about the STI master’s programs and an academic calendar for the STI Cohort 2013 option. Please contact us at info@sans.edu if you have any questions about STI or the STI Cohort 2013. In addition to the STI Cohort 2013 option, STI also has a standard option which allows a student to take up to five years to complete the master’s program and provides flexibility regarding course locations and delivery methods.

The master’s degree programs provide a comprehensive array of courses that allow students to gain technical mastery of technologies and processes that set apart the leading security practitioners in the field. Equally important are the additional courses and special programs the degree offers that enable students to master communications, project management, presenting, mentoring, and persuasive skills. We help you develop your reputation in the industry by ensuring your work is published through our online repositories including the SANS Reading Room and Policy project, STI Student Presentations, Student Projects, and Leadership Lab. The degree candidates will have the opportunity to study with excellent members of faculty, many of whom have written the books that other security programs use to direct their courses. Many on the faculty hold Ph.D. and master’s degrees from institutions like MIT, Carnegie Mellon, and other leading schools. We look forward to having you apply to STI. Please contact us if you have any questions.

Best regards,

Stephen Northcutt
President
# Table of Contents

A Letter from the President ................................................................. 2  
Table of Contents ............................................................................. 3  
STI Cohort 2013 ................................................................................. 4, 5  
Academic Calendar ........................................................................... 6, 7  
About SANS Technology Institute (STI) ............................................ 8, 9  
  Authorization .................................................................................. 8  
  Why Choose STI ............................................................................ 8  
  Admissions Requirements ............................................................. 8  
  Transfers ....................................................................................... 8  
  How to Apply ............................................................................... 9  
  Transcripts ................................................................................... 9  
  Tuition and Fees ........................................................................... 9  
Degree Programs and Curricula ....................................................... 10  
Master of Science Degree in Information Security Management ........ 11  
Master of Science Degree in Information Security Engineering .......... 12  
Course Descriptions ........................................................................ 13, 14, 15  
  SEC401: SANS Security Essentials Bootcamp Style ...................... 13  
  SEC503: Intrusion Detection In-Depth ........................................... 13  
  SEC504: Hacker Techniques, Exploits, and Incident Handling ........ 13  
  FOR408: Computer Forensic Investigations - Windows In-Depth ...... 13  
  FOR508: Advanced Computer Forensic Analysis and Incident Response 13  
  FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Technique 13  
  MGT305: Technical Communication and Presentation Skills for Security Professionals 13  
  MGT411: SANS 27000 Implementation & Management .................... 13  
  MGT421: SANS Leadership and Management Competencies ............. 14  
  MGT438: How to Establish a Security Awareness Program ............... 14  
  MGT512: SANS Security Leadership Essentials for Managers with Knowledge Compression™ 14  
  MGT525: Project Management and Effective Communications for Security Professionals and Managers 14  
  LEGS23: Law of Data Security and Investigations ......................... 14  
  DEV522: Defending Web Applications Security Essentials ............... 14  
  DEV536: Secure Coding for PCI Compliance .................................... 15  
  DEV541: Secure Coding in Java/JEE: Developing Defensible Applications 15  
  DEV542: Web App Penetration Testing and Ethical Hacking ............ 15  
  DEV544: Secure Coding in .NET: Developing Defensible Applications 15  
  AUD507: Auditing Networks, Perimeters & Systems ....................... 15  
Community Project Requirements ................................................... 16, 17  
  Work Study .................................................................................. 16  
  Group Discussion and Written Project ............................................ 16  
  Presentations ............................................................................... 17  
  Joint Written Project ................................................................. 17  
  GSE ......................................................................................... 17  
  Teaching Assistant .................................................................... 17  
  Awareness Talk to Community ..................................................... 17  
Faculty .......................................................................................... 18  
Application Form .............................................................................. 19, 20  
Employer Endorsement Form .......................................................... 21, 22  
Student Declaration Form ............................................................... 23, 24
The STI Cohort 2013 is an accelerated option in the Washington, DC Metro area, for students to earn a Master of Science in Information Security Management (MSISM) or a Master of Science in Information Security Engineering (MSISE) in two years.

We use the word Cohort to mean a group of STI students who take classes together and who graduate at the same time. A cohort results in increased opportunities for students to develop beneficial relationships that can last for years to come.

There is an immediate need for highly qualified information security professionals in both the government and private sector. The SANS Technology Institute (STI) offers intensive, hands-on programs with a focus on information security engineering or information security management that will arm you with leadership skills as well as the knowledge and expertise necessary to help you to obtain top information security management positions in government and private industries.

STI Cohort 2013 students will:
· Earn a master’s degree in two years, starting April 15, 2011
· Enter the program, complete courses, perform Community Project Requirements, and graduate with the same group of students
· Benefit from a strong, hands-on learning environment
· Build beneficial relationships for the future
· Be able to apply their knowledge to their job immediately
· Need the endorsement of their employer

Apply Now!
STI Cohort 2013 is limited to 50 students.
Applications must be received by April 1, 2011.
Classes for the STI Cohort 2013 begin April 15, 2011 in the Washington, DC Metro area.
# Academic Calendar

## STI Cohort 2013 Academic Calendar

<table>
<thead>
<tr>
<th>Event</th>
<th>Date</th>
<th>MSISM Curriculum</th>
<th>MSISE Curriculum</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>MGT512: SANS Security Leadership Essentials For Managers with Knowledge Compression™</td>
<td>SEC401: SANS Security Essentials Bootcamp Style</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>May 2011</td>
<td>GSLC Gold Paper</td>
<td>GSEC Gold Paper</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Work Study*</td>
<td>Work Study*</td>
</tr>
<tr>
<td></td>
<td>July 2011</td>
<td>GCIH Gold Paper</td>
<td>GCIH Gold Paper</td>
</tr>
<tr>
<td></td>
<td>August 2011</td>
<td>Time to complete Gold Papers</td>
<td>Time to complete Gold Papers</td>
</tr>
<tr>
<td>OnDemand Online Training</td>
<td>Sept 2011</td>
<td>MGT421: SANS Leadership and Management Competencies (Written Assignment)</td>
<td>MGT421: SANS Leadership and Management Competencies (Written Assignment)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Submit Presentation Proposal</td>
<td>Submit Presentation Proposal</td>
</tr>
<tr>
<td>OnDemand Online Training</td>
<td>Oct 2011</td>
<td>MGT404: Fundamentals of Information Security Policy (Course may be lengthened)</td>
<td>MGT404: Fundamentals of Information Security Policy (Course may be lengthened)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MGT438: How to Establish a Security Awareness Program (Course may be lengthened) (Written Assignment)</td>
<td>MGT438: How to Establish a Security Awareness Program (Course may be lengthened) (Written Assignment)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Work on Presentation</td>
<td>Work on Presentation</td>
</tr>
<tr>
<td></td>
<td>Nov 2011</td>
<td>Finalize Presentation</td>
<td>Finalize Presentation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Complete Written Assignments</td>
<td>Complete Written Assignments</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1st Evening Presentation</td>
<td>1st Evening Presentation</td>
</tr>
<tr>
<td></td>
<td>Jan 2012</td>
<td>GCPM Gold Paper</td>
<td>GCPM Gold Paper</td>
</tr>
<tr>
<td></td>
<td>Feb 2012</td>
<td>Joint Written Project</td>
<td>Joint Written Project</td>
</tr>
<tr>
<td></td>
<td>March 2012</td>
<td>Finalize Joint Written Project</td>
<td>Finalize Joint Written Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Complete GCPM Gold Paper</td>
<td>Complete GCPM Gold Paper</td>
</tr>
</tbody>
</table>

*If there are not enough slots available to do the Work Study Community Project Requirement (CPR) or Teaching Assistant where indicated in the chart above, the student will perform those CPRs at a different training event. STI Cohort 2013 students should plan on attending the courses listed above, but if you are unable to attend a course, you can be part of the class by taking it through SANS Simulcast.*
## STI Cohort 2013 Academic Calendar (continued)

<table>
<thead>
<tr>
<th>Event</th>
<th>Date</th>
<th>MSISM Curriculum</th>
<th>MSISE Curriculum</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Northern Virginia 2012</td>
<td>April 2012</td>
<td>Group Discussion and Written Project</td>
<td>Group Discussion and Written Project</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>AUD507</strong>: Auditing Networks, Perimeters, and Systems</td>
<td><strong>SEC503</strong>: Intrusion Detection In-Depth</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GSNA Gold Paper</td>
<td>GCIA Gold Paper</td>
</tr>
<tr>
<td></td>
<td>May 2012</td>
<td>Complete GSNA Gold Paper</td>
<td>Complete GCIA Gold Paper</td>
</tr>
<tr>
<td>SANSFIRE 2012</td>
<td>June 2012</td>
<td>LEG523: Law of Data Security and Investigations</td>
<td>Elective #1</td>
</tr>
<tr>
<td>Washington, DC</td>
<td></td>
<td></td>
<td>GSE</td>
</tr>
<tr>
<td></td>
<td>July 2012</td>
<td>GLEG Gold Paper</td>
<td></td>
</tr>
<tr>
<td></td>
<td>August 2012</td>
<td>Complete GLEG Gold Paper</td>
<td>Complete GCIA or GCPM Gold Paper</td>
</tr>
<tr>
<td>SANS NS 2012</td>
<td>Sept 2012</td>
<td>Teaching Assistant* (part of Cohort) or Software Security</td>
<td>Submit Presentation Proposal</td>
</tr>
<tr>
<td>Las Vegas, NV</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Oct 2012</td>
<td>If you take Software Security, then complete Gold Certifications</td>
<td>Work on Presentation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Work on Presentation</td>
<td></td>
</tr>
<tr>
<td>SANS CDI 2012</td>
<td>Dec 2012</td>
<td>Teaching Assistant* (part of Cohort)</td>
<td><strong>FOR508</strong>: Advanced Computer Forensic Analysis and Incident Response</td>
</tr>
<tr>
<td>Washington, DC</td>
<td></td>
<td>OR Software Security</td>
<td>OR Software Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Start Software Security Golds (if not complete)</td>
<td>2nd Evening Presentation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2nd Evening Presentation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Jan 2013</td>
<td><strong>MGT411</strong>: SANS 27000 Implementation and Management</td>
<td>GCFA Gold Paper or Software Security Gold Paper</td>
</tr>
<tr>
<td></td>
<td>Feb 2013</td>
<td>G7799 Gold Paper OR Software Security Golds (if not complete)</td>
<td>Complete GCFA Gold Paper</td>
</tr>
<tr>
<td></td>
<td>March 2013</td>
<td>Plan/Work on Security Awareness Presentation</td>
<td>Plan/Work on Security Awareness Presentation</td>
</tr>
<tr>
<td>SANS Northern Virginia 2013</td>
<td>April 2013</td>
<td>Complete G7799 Gold Paper and Software Security Golds (if not complete)</td>
<td>Elective #2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Awareness Presentation; Graduate Exit Interview</td>
<td>Security Awareness Presentation; Graduate Exit Interview</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Awareness Presentation</td>
<td>Security Awareness Presentation</td>
</tr>
<tr>
<td>SANSFIRE 2013</td>
<td>June 2013</td>
<td><strong>Graduation – Formal Ceremony</strong></td>
<td><strong>Graduation – Formal Ceremony</strong></td>
</tr>
<tr>
<td>Washington, DC or Baltimore, MD</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
About SANS Technology Institute (STI)

STI seeks to prepare the next generation of information security leaders for what they will face. Two growing trends will shape cyber security in the future: increasing interest by organized crime that is accompanying the growth of e-commerce and e-government, and the increasing impact of cyber methods of warfare. These forces will contribute to an already massive and continually growing need for thousands of new technical cyber security managers.

STI is affiliated with the SANS Institute, the most trusted and by far the largest source for information security training in the world. STI is also affiliated with GIAC (Global Information Assurance Certification) which is trusted by thousands of companies and government agencies. The mission of STI is to develop the information security technology leaders needed to help strengthen the information community all over the world by improving the security of cyberspace. STI seeks to prepare both the managers of information security groups and the technical leaders who direct security technology programs. STI’s primary functional emphasis is instruction, but the Institute’s faculty and students will engage in research and public service programs.

Authorization

SANS Technology Institute is authorized by the Maryland Higher Education Commission to grant the Master of Science Degrees in Information Security Engineering and Information Security Management. SANS Technology Institute is a Candidate for Accreditation by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104. (267-284-5000). Candidate for Accreditation is a status of affiliation with a regional accrediting commission which indicates that an institution has achieved initial recognition and is progressing toward, but is not assured of, accreditation. It has provided evidence of sound planning, appears to have the resources to implement the plans, and appears to have the potential for reaching its goals within a reasonable time. Candidate for Accreditation status was granted in March 2010.

Why Choose STI

- STI’s master’s degree programs provide a comprehensive array of courses to help students gain technical mastery of technologies and processes
- Community Project Requirements (CPRs) enable students to master communications, project management, presenting, mentoring, and persuasive skills
- STI helps you develop your reputation in the industry by ensuring your work is published through our online repositories, including the SANS Reading Room and Security Policy Project, STI Projects at www.sans.edu/resources/student_projects, STI presentations at www.sans.edu/resources/student_presentations, and STI Leadership Lab at www.sans.edu/resources/leadership_lab
- STI faculty members are experts in the information security field with practical, current knowledge

Admissions Requirements

- A baccalaureate degree from a recognized college or university, or equivalent international education, with a minimum cumulative grade point average of 2.8. There are two exceptions to the 2.8 minimum described on the Web site. Your baccalaureate does not have to be in the field of information security/information technology.
- At least 12 months of experience in the field.
- Upon completion of the program, you will have three years of significant work experience in information technology, security or audit. If you are already working in the field, this should not be a problem.

Transfers

Applicants can transfer in GIAC certifications that are related to the master’s curriculum, that are current, and have scores of 80 (or average of 80 if applicable) or higher.
How to Apply

• Complete the application form in the back of this brochure, or you can download one at www.sans.edu/downloads/application.pdf. **Make a note with your application that you are applying for the STI Cohort 2013 option.**

• Include a nonrefundable application fee of $450.00 with your completed application.

• Have official transcripts sent directly from the college or university that awarded your baccalaureate degree, or equivalent international degree, to STI.

• Submit a letter of recommendation from your employer (the form is downloadable at www.sans.edu/downloads/recommendation.pdf, and the Employer Endorsement form in the back of this brochure.

• Submit a resume of your related experience in the field.

• Submit an outcome statement. This should be a one sentence (but better to also provide background information) to two-page typed paper stating what you expect the outcome of your life will be after making the investment to complete an STI master’s program.

• Submit Leadership Essay
  - **Part A:**
    Write a leadership essay describing leadership qualities you have demonstrated in the past. You must read the following article but it is perfectly acceptable to refer to a competency that is not listed in the article at www.sans.edu/resources/leadershiplab/sti_leadership_essay.php
  - **Part B:**
    Start a new page, and list three competencies that you want to work on. You must read the following article but it is perfectly acceptable to refer to a competency that is not listed in the article at www.sans.edu/resources/leadershiplab/sti_leadership_essay.php

  We are looking at the quality of the writing (content, grammar, spelling, etc.) since one of the characteristics of being a leader is being able to write well.

• Submit Student Declaration form in the back of this brochure

• **Application deadline is April 1, 2011**

  For STI Cohort 2013 only, submit an Employer Endorsement Form and Student Declaration Form available in the back of this brochure or download at www.sans.edu/programs/sti-cohort-2013/apply.php

The completed application for admission and supporting credentials should be directed to:

**SANS Technology Institute Master's Program Registration**
8120 Woodmont Avenue, Suite 205
Bethesda, Maryland 20814

Also, in addition to mailing hard copies of your essays and resume, please e-mail the essays and resume to info@sans.edu in the form of separate document attachments.

Transcripts

Transcripts must be sent directly to STI by the granting institution. Employers may send their recommendation separately, but all other documents should be in the package you send. The application package will be considered complete for review once STI has obtained all required materials, and all credentials become property of STI.

Tuition and Fees

Estimated total cost to complete the master’s programs is approximately: $29,000 to $33,000.

Tuition for credit seeking courses is the same as any other SANS course with GIAC certification (www.giac.org) and must be paid in full prior to the beginning of each course. Payment for attempting the Gold certification is made when you start the Gold process. For more information about scheduling, or costs, please see www.sans.org. For information about Gold, see www.giac.org/gold.

At present, there are no additional tuition costs related to a student’s Community Project Requirement experiences. Students are responsible for the costs of hotel, food, and travel for the residential institutes except that the institution, pays for the hotel room when an MSISM student performs Teaching Assistant Duty as a Community Project Requirement.
Degree Programs and Curricula

**STI Master of Science degree programs offer candidates an unparalleled opportunity to excel in the two aspects of security that are most important to the success of their employer and their own careers.**

Technical mastery comes from the combination of:

1. An uncompromising, research-based technical curriculum that allows you to master the most current threats, the most effective techniques to block them, the underlying principles on which those techniques are based, and the leading edge of research in each area.

2. A faculty that includes highly-rated instructors in the security field – people who have written the best-selling books, people who are shaping the future of security, people who bring practical, real-world experience and case studies to the class and help you gain confidence in your mastery; and

3. Research assignments that involve you in current, important areas of security, and enable you to publish research that can help move the field forward.

The second area in which STI degree programs help you excel is in management skills that are so often lacking in otherwise effective technical professionals. Technology initiatives, and particularly security initiatives, are too often destined to fail because of missing management and communication skills. Both programs are writing intensive with technical research papers required for most courses.

Management skills that are central to success in information security include:

- Effective advocacy of information security
- Management and leadership skills
- Project budgeting
- Project management in information technology
- Effective spoken and written communication
- Presenting and mentoring skills

These skills are taught in special courses, but they are also reinforced in special add-on activities that are woven into other courses and community project requirements that the student takes.
Master of Science Degree in Information Security Management (MSISM)

The MSISM (Management) Program is designed to help a candidate become the highest-ranking management employee with IT Security responsibilities in an organization. In the government, this is often called the designated approving authority, or information assurance manager (IAM). In the industry, titles such as chief security officer or chief information security officer are often used. In addition to the strong writing skills the program produces through the GIAC Gold program or the Writing Assignments for almost all courses, the Community Project Requirements training includes teamwork and oral presentation practice. More information about GIAC Gold can be found at www.giac.org.

Core Courses

<table>
<thead>
<tr>
<th>Course</th>
<th>Certification</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGT305: Technical Communication &amp; Presentation Skills for Security Professionals</td>
<td>Assessment</td>
<td>1</td>
</tr>
<tr>
<td>MGT512: SANS Security Leadership Essentials For Managers with Knowledge Compression™</td>
<td>GSLC Gold</td>
<td>3</td>
</tr>
<tr>
<td>SEC504: Hacker Techniques, Exploits, and Incident Handling</td>
<td>GCIH Gold</td>
<td>4</td>
</tr>
<tr>
<td>MGT525: Project Management and Effective Communications for Security Professionals and Managers</td>
<td>GCPM Gold</td>
<td>4</td>
</tr>
<tr>
<td>AUD507: Auditing Networks, Perimeters, and Systems OR CISA exam and a Written Assignment</td>
<td>GSNA Gold</td>
<td>4</td>
</tr>
<tr>
<td>MGT404: Fundamentals of Information Security Policy (course may be lengthened)</td>
<td>Substitute for Exam, Written Assignment</td>
<td>1</td>
</tr>
<tr>
<td>MGT438: How to Establish a Security Awareness Program (course may be lengthened)</td>
<td>Substitute for Exam, Written Assignment</td>
<td>1</td>
</tr>
<tr>
<td>MGT421: SANS Leadership and Management Competencies</td>
<td>Substitute for Exam, Written Assignment</td>
<td>1</td>
</tr>
<tr>
<td>LEG523: Law of Data Security and Investigations</td>
<td>GLEG Gold</td>
<td>3</td>
</tr>
<tr>
<td>MGT411: SANS 27000 Implementation &amp; Management</td>
<td>G7799 Gold</td>
<td>4</td>
</tr>
</tbody>
</table>

Software Security
(At least 6 days of courses), Gold Certs or Written Assignments if Gold not available – Four credits

<table>
<thead>
<tr>
<th>Course</th>
<th>Certification</th>
<th>Days</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEV522: Defending Web Application Security Essentials</td>
<td>Exam if avail or sub</td>
<td>6 days</td>
</tr>
<tr>
<td>DEV541: Secure Coding in Java/JEE: Developing Defensible Applications</td>
<td>GSSP-JAVA</td>
<td>4 days</td>
</tr>
<tr>
<td>DEV542: Web App Penetration Testing &amp; Ethical Hacking</td>
<td>GWAPT</td>
<td>6 days</td>
</tr>
<tr>
<td>DEV536: Secure Coding for PCI Compliance</td>
<td>Exam if avail or sub</td>
<td>2 days</td>
</tr>
<tr>
<td>DEV544: Secure Coding in .Net: Developing Defensible Applications</td>
<td>Exam if avail or sub</td>
<td>4 days</td>
</tr>
</tbody>
</table>

Community Project Requirements
(Seven CPRs) – Three credits

TOTAL CREDITS 33
Master of Science Degree in Information Security Engineering Curriculum (MSISE)

This MSISE (Engineering) Program will prepare students to head teams of technologists who are responsible for information security assessments, architectures, operations, monitoring, auditing, and lead information security programs. Graduates will be qualified to seek positions such as technical director for information security, senior security analyst, senior security administrator, information systems security manager, information systems security officer, information security manager, and chief information security officer. The program focuses primarily on the technical and problem-solving skills associated with security implementation, but adds instruction on project management and effective communications to help graduates prepare to take responsibility for the work of other technologists. Almost all of the courses below, except the electives, include writing assignments called GIAC Gold or Written Assignment. More information about GIAC Gold can be found at www.giac.org.

### Core Courses

<table>
<thead>
<tr>
<th>Course</th>
<th>Certification</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGT305: Technical Communication &amp; Presentation Skills for Security Professionals</td>
<td>Assessment</td>
<td>1</td>
</tr>
<tr>
<td>SEC401: SANS Security Essentials Bootcamp Style</td>
<td>GSEC Gold</td>
<td>4</td>
</tr>
<tr>
<td>SEC504: Hacker Techniques, Exploits, and Incident Handling</td>
<td>GCIH Gold</td>
<td>4</td>
</tr>
<tr>
<td>MGT525: Project Management and Effective Communications for Security Professionals and Managers</td>
<td>GCPM Gold</td>
<td>4</td>
</tr>
<tr>
<td>SEC503: Intrusion Detection In-Depth</td>
<td>GCIA Gold</td>
<td>4</td>
</tr>
<tr>
<td>FOR508: Advanced Computer Forensic Analysis and Incident Response OR Software Security Training see <a href="http://www.sans.edu/programs/msise">www.sans.edu/programs/msise</a></td>
<td>GCFA Gold, GIAC Gold</td>
<td>4</td>
</tr>
<tr>
<td>MGT404: Fundamentals of Information Security Policy (course may be lengthened)</td>
<td>Substitute for Exam, Written Assignment</td>
<td>1</td>
</tr>
<tr>
<td>MGT438: How to Establish a Security Awareness Program (course may be lengthened)</td>
<td>Substitute for Exam, Written Assignment</td>
<td>1</td>
</tr>
<tr>
<td>MGT421: SANS Leadership and Management Competencies</td>
<td>Substitute for Exam, Written Assignment</td>
<td>1</td>
</tr>
</tbody>
</table>

### Two Electives

(No gold required from the following options) – Six credits

For students interested in Forensics, we have established a “Forensics Focus” that allows students to take the following courses for their elective requirement:

<table>
<thead>
<tr>
<th>Course</th>
<th>Certification</th>
<th>Days</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOR408: Computer Forensic Essentials</td>
<td>GCFE – no paper</td>
<td>3</td>
</tr>
<tr>
<td>FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques</td>
<td>GREM – no paper</td>
<td>3</td>
</tr>
</tbody>
</table>

Or students who do not wish to pursue the “Forensics Focus” can choose two elective courses with at least one being a major SEC/DEV 500/600/700 level, GIAC Certification. Students can choose the other elective from the following:

<table>
<thead>
<tr>
<th>Course</th>
<th>Certification</th>
<th>Days</th>
</tr>
</thead>
<tbody>
<tr>
<td>Another major SEC/DEV500/600/700 level course</td>
<td>GIAC Cert</td>
<td>3</td>
</tr>
<tr>
<td>AUD507: Auditing Networks, Perimeters, and Systems</td>
<td>GSNA Gold</td>
<td>3</td>
</tr>
</tbody>
</table>

### Community Project Requirements (Seven CPRs) – Three credits

TOTAL CREDITS 33
SEC401: SANS Security Essentials Bootcamp Style
SANS Security Essentials is designed to give anyone interested in network security the skills required to be an effective player in this arena. This in-depth, comprehensive course provides the essential, up-to-the-minute knowledge and skills required for securing systems and organizations, and equips you with the language and theory of computer security. Learn all of this and more from the best security instructors in the industry.

SEC503: Intrusion Detection In-Depth
The emphasis of this course is on increasing students’ understanding of the workings of TCP/IP, methods of network traffic analysis, and one specific network intrusion detection system (NIDS) – Snort. This is not a comparison or demonstration of multiple NIDSs. Instead, the knowledge provided here allows students to better understand the qualities that go into a sound NIDS and the whys behind them, and thus, to be better equipped to make a wise selection for their site’s particular needs. This is a fast-paced course, and students are expected to have a basic working knowledge of TCP/IP in order to fully understand the topics that will be discussed. We strongly recommend that you spend some time getting familiar with TCPdump, WinDump, or another network analyzer output before coming to class.

Prerequisite: Students must possess at least a working knowledge of TCP/IP & Hex.

SEC504: Hacker Techniques, Exploits, and Incident Handling
This course addresses the latest cutting-edge insidious attack vectors and the “oldie-but-goodie” attacks that are still so prevalent, and everything in between. Instead of merely teaching a few hack-attack tricks, this course includes a time-tested, step-by-step process for responding to computer incidents; a detailed description of how attackers undermine systems so you can prepare, detect, and respond to them; and a hands-on workshop for discovering holes before the bad guys do. Additionally, the course explores the legal issues associated with responding to computer attacks, including employee monitoring, working with law enforcement, and handling evidence.

FOR408: Computer Forensic Investigations - Windows In-Depth
This course focuses on the critical knowledge that a computer forensic investigator must know to investigate computer crime incidents successfully. You will learn how computer forensic analysts focus on collecting and analyzing data from computer systems to track user-based activity that could be used internally or in civil/criminal litigation. In addition to in-depth technical digital forensic knowledge on Windows Digital Forensics (Windows XP through Windows 7 and Server 2008), you will be exposed to well known computer forensic tools such as FTK, Registry Analyzer, FTK Imager, Prefetch Analyzer, and much more.

FOR508: Advanced Computer Forensic Analysis and Incident Response
This course will give you a firm understanding of advanced incident response and computer forensics tools and techniques to investigate data breach intrusions, tech-savvy rogue employees, advanced persistent threats, and complex digital forensic cases. This course will also teach you critical forensic analysis techniques and tools in a hands-on setting for both Windows and Linux-based investigations.

FOR610: Reverse-Engineering Malware: Malware Analysis Tools and Techniques
This popular malware analysis course has helped forensic investigators, malware specialists, incident responders, and IT administrators assess malware threats. The course teaches a practical approach to examining malicious programs (spyware, bots, trojans, etc.) that target or run on Microsoft Windows. This training also looks at reversing Web-based malware, such as JavaScript and Flash files, as well as malicious document files. By the end of the course, you’ll learn how to reverse-engineer malicious software using a variety of system and network monitoring utilities, a disassembler, a debugger, and other tools for turning malware inside-out.

MGT305: Technical Communication and Presentation Skills for Security Professionals
This course covers the top techniques that will show any student how to research and write professional quality reports, how to create outstanding presentation materials, and as an added bonus, how to write expert witness reports. Students will also get a crash course on advanced public speaking skills.

MGT404: Fundamentals of Information Security Policy
The Fundamentals of Information Security Policy course focuses on how to write, analyze and assess a wide range of security policies, including issue and system-specific policy. The student will develop skills and practical experience by completing the 24 guided labs that cover both the policy header and policy body or statement, and learn to create successful policy that is accepted by the organization by being sensitive to the corporate culture. This is a hands-on, exercise-intensive course on writing, implementing and assessing security policies. (This course may be lengthened)

MGT411: SANS 27000 Implementation & Management
This course is designed for information security officers or other management professionals who are looking for a how-to guide for implementing ISO-27000 effectively and quickly. While the standard is very well written, anyone who has actually tried to shift to an ISO-27000 structured security organization knows that there can be some significant hurdles to overcome.

Find detailed course descriptions at www.sans.org
Course Descriptions

MGT421: SANS Leadership and Management Competencies
This course is designed to develop existing and new supervisors and managers who aspire to go beyond being the boss. It will help you build leadership skills to enhance the organization’s climate and team-building skills to support the organization’s mission, its growth in productivity, workplace attitude/satisfaction, and staff and customer relationships.

MGT438: How to Establish a Security Awareness Program
This course is based on NIST SP 800-50, "Building an Information Technology Security Awareness and Training Program." Being able to design, implement, and manage an effective security awareness program is difficult at best. This course walks security managers through the architecture and design of a successful security awareness program and helps the student to document and design a clear cut strategy, approach, and implementation plan. *(This course may be lengthened)*

MGT512: SANS Security Leadership Essentials for Managers with Knowledge Compression™
This course is designed to empower advancing managers who want to get up to speed quickly on information security issues and terminology. Essential security topics covered in this management course include: network fundamentals and applications, power, cooling and safety, architectural approaches to defense in-depth, cyber attacks, vulnerability assessment and management, security policies, contingency and continuity planning, awareness management, risk management analysis, incident handling, Web application security, offensive and defensive information warfare, culminating with our management practicum.

MGT525: Project Management and Effective Communications for Security Professionals and Managers
The project management process is broken down into core process groups that can be applied across multiple areas of any project. Keeping in line with prevalent needs from the InfoSec industry, we look at projects that create and maintain services and cover in depth how cost, time, quality, and risk affect IT security and the services we provide to others both inside and outside of our organizational boundaries. We go into great detail covering human resource management as well as effective communication and conflict resolution. People are the most valuable resource we have on a project, and the communication and conflict resolution techniques presented can be used in all areas of professional work. Above all, projects fail or succeed because of the people involved. You want to make sure the people involved with the development and execution of your project build a strong team and communicate effectively.

LEG523: Law of Data Security and Investigations
This course covers the law of business, contracts, fraud, crime, IT security, IT liability, and IT policy – all with a focus on electronically stored and transmitted records. Topics include: Fundamentals of IT Security Law and Policy; E-Records, E-Discovery and Business Law; Contracting for Data Security; The Law of IT Compliance: How to Conduct Investigations and Applying Law to Emerging Dangers: Cyber Defense.

DEV522: Defending Web Applications Security Essentials
This course covers the OWASP Top 10 and will help you to better understand Web application vulnerabilities, thus enabling you to properly defend your organization’s Web assets. Mitigation strategies from an infrastructure, architecture, and coding perspective will be discussed alongside real-world implementations that really work. The testing aspect of vulnerabilities will also be covered so you can ensure your application is tested for the vulnerabilities discussed in class. The class goes beyond classic Web applications and includes coverage of Web 2.0 technologies like AJAX and Web services.
DEV536: Secure Coding for PCI Compliance
Throughout the course we will look at examples of the types of flaws that secure coding protects against, examine how the flaw might be exploited and then focus on how to correct that code. Coupled with the lectures, there are more than ten hands-on exercises where students will have the opportunity to test out their new skills: identifying flaws in code; fixing code; and writing secure code. All of the exercises are available in Perl, PHP, C/C++, Ruby, and Java. This will allow the student to try their hand at any of the major Web application coding languages that they work with in addition to some of the supporting languages that might be at work behind the scenes. Students are not required to be familiar with all of these languages but should be proficient in at least one of them. Lectures are presented using a more or less code-neutral format.

DEV541: Secure Coding in Java/JEE: Developing Defensible Applications
In this course, you will examine actual code, work with real tools, build applications, and gain confidence in the resources you need for the journey to improving the security of Java applications. Rather than teaching students to use a set of tools, we’re teaching students concepts of secure programming. This involves looking at a specific piece of code, identifying a security flaw, and implementing a fix for flaws found on the Top 10 and CWE/SANS Top 25 Most Dangerous Programming Errors. The class culminates in a Secure Development Challenge where you perform a security review of a real-world open-source application. You will conduct a code review, perform security testing to actually exploit real vulnerabilities, and finally, using the secure coding techniques that you have learned in class and implement fixes for these issues.

DEV/SEC542: Web App Penetration Testing and Ethical Hacking
In this intermediate to advanced level class, students learn the art of exploiting Web applications so they can find flaws in Web apps before the bad guys do. Through detailed, hands-on exercises and training from a seasoned professional, students are taught the four-step process for Web application penetration testing. Exercises include injecting SQL into back-end databases, learning how attackers exfiltrate sensitive data, utilizing cross-site scripting attacks to dominate a target infrastructure in our unique hands-on laboratory environment, and exploring various other Web app vulnerabilities in depth with tried-and-true techniques for finding them using a structured testing regimen.

DEV544: Secure Coding in .NET: Developing Defensible Applications
This course analyzes the defensive strategies and technical underpinnings of the ASP.NET framework and teaches students where to leverage defensive technologies in the framework, and where to build security in by hand. This course also examines strategies for building applications that will be secure both today and in the future.

AUD507: Auditing Networks, Perimeters, and Systems
This course is organized specifically to provide a risk driven-method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high-level audit issues and general audit best practice, the students will have the opportunity to dive deep into the technical how-to for determining the key controls that can be used to provide a level of assurance to an organization. Tips on how to repeatedly verify these controls and techniques for automatic compliance validation will be given from real-world examples.

Find detailed course descriptions at www.sans.org
Community Project Requirements (CPRs)

A SANS Technology Institute education provides opportunities for you to build your own network of security professionals with the other students and the faculty. The projects, which involve research, writing and presenting, are graded. The sum of your scores on these exercises will be your final Community Project grade; or, if they are graded on a pass/fail basis, you must pass each exercise to receive a passing Community Project Requirements grade.

Residential Institutes and Community Project Requirements

All STI students are required to attend at least three Residential Institutes (RI), large six-day conferences that the SANS Institute offers on a periodic basis in various U.S. cities and some international sites.

Community Project Requirements that must be performed at Residential Institutes

- Work Study
- Group Discussion & Written Project – you will arrive two days before the RI to work on a presentation with your peers. Topics will be assigned the first day and presented on the second day. Due to a timing conflict, it is unlikely that Work Study and the Group Discussion & Written Project can be performed at the same RI.
- Two presentations
- GSE for MSISE Students/Teaching Assistant for MSISM students

Community Project Requirements not performed at Residential Institutes

- Joint Written Project
- Awareness Talk to Community

Work Study

Master’s students are required to participate as a facilitator in the Work Study program for their first Community Project Requirement. To be eligible to apply for Work Study as a Community Project Requirement, the student must have attended a large SANS training event in the past. In addition to attending class, you will be part of a live SANS conference. The purposes of Work Study are to help build leadership skills, team building skills, and, as a side benefit, you will probably develop relationships that last for years.

Students must write an essay about their Work Study experience and what they learned about leadership.

NOTE: Work Study opportunities are limited so you should apply for Work Study well in advance.

Group Discussion and Written Project*

Students will arrive two days before the event starts to participate in a Group Discussion and Written Project (GDWP). A problem will be presented to the student’s team the evening before the project is to be presented; and, as a team, the team prepares to present a recommended solution to senior staff about 24 hours later. As a leader, you will be expected to deal with situations with short turnaround times, so this project allows you to demonstrate those skills and to improve them. The team will select one member to give the presentation. The presentation will be 15 minutes, 7 slides, 5 to 6 bullets per slide, maximum 10 typed pages. The presentation usually occurs during the evening to a member of STI’s senior staff. Generally, there are no other people in the audience, or only a few. The grade will be a team grade/each student in that team will receive the same grade.
Presentations*

Students must make two presentations at two of the RIs. The presentation topic is based on the student’s previously earned GIAC Gold certifications research (unless the student receives permission from the college to use a topic not related to Gold). Students may request resource material about “How to Give Effective Presentations” by e-mailing info@sans.edu – see www.sans.edu/resources for more information. The presentation will be given in front of an STI senior staff member. Generally, it is performed in the evening, with additional people in the audience. Presentations are to be 30 minutes long with an extra 7 to 10 minutes for questions: 15 slides with notes - 1st is title, 2nd is objective, 12 are content, last is summary; 5 to 6 bullets per slide. You must use the template that can be obtained by contacting info@sans.edu.

Joint Written Project*

A student must engage in one Joint Written Project (JWP) during the term of the master’s program. It is recommended, but not required, that the student take MGT525: Project Management and Effective Communications for Security Professionals and Managers before the student starts the Joint Written Project. The student must work with at least one other student as his or her partner(s) in the JWP. The grading rubric is provided at www.sans.edu/programs/grading-rubrics.php. The JWP is written, and does not involve an oral presentation. The students will collaborate with their partner(s) by e-mail, phone, etc. to coordinate their efforts. In life, partners often must coordinate a project by e-mail, phone, etc. rather than face-to-face, so this project gives students experience working virtually. After the students receive the topic, they have up to 7 calendar days to submit their Project Plan for review. Once the Project Plan is approved, they have 30 days to submit the completed project for grading to the SANS Technology Institute. The grade will be a team grade; each student in that team will receive the same grade. The grade will be on a pass/fail basis, but that may change in the future. SANS Technology Institute may, but is not required to, post passing projects onto its Web site.

GSE – MSISE Program

MSISE students must pass the GIAC GSE. The GSE exam is given in two parts. The first part is a multiple choice exam which may be taken at a proctored location, just like any other GIAC exam. The current version of the GSE multiple choice exam has the passing score set at 75%, and the time limit is 3 hours. Passing this exam qualifies a person to sit for the GSE hands-on lab. The first day of the two day GSE lab consists of a rigorous battery of hands-on exercises drawn from many domains. The second day consists of an Incident Response Scenario that requires the candidate to analyze data and report their results in a written incident report.

Teaching Assistant – MSISM Program

As one of the last Community Project Requirements, students in the MSISM program will assist an instructor as a teaching assistant in a hands-on course. Leaders have to be good at troubleshooting, whether the problem is technical, process or personal. A teaching assistant’s job is to help other students, and that usually involves a lot of troubleshooting. The student will benefit from being exposed to an excellent hands-on instructor, and the student will be able to exercise important skills while assisting others in the hands-on instruction.

Awareness Talk to Community

Within 30 days after the student finishes the presentations and projects described above, the student must present a plan to SANS Technology Institute describing how the student intends to satisfy the Awareness Talk at little or no cost to the community. The student must give the talk within a reasonable time after the plan is approved.

*Students are required to take and pass MGT305: Technical Communication & Presentation Skills & Assessment before completing the noted CPRs
At the SANS Technology Institute, you learn security from the top experts in the field, the authors of the most authoritative books, and, most importantly, from people who have front line, in-the-trenches experience doing the types of jobs that you will be required to do. Below are just a few of our distinguished faculty members. To see a complete list and read faculty bios, please visit www.sans.edu/faculty.

Tanya Baccam  
B.S., SANS Senior Certified Instructor.  
B.S., Dordt College

Eric Cole  
Ph.D., Department Chair, Faculty, SANS Fellow.  
M.S., NYIT, Ph.D., Pace University

Jason Fossen  
M.S., Faculty, SANS Fellow.  
M.S., University of Texas at Austin

Jeff Frisk  
B.S., Faculty, SANS Certified Instructor.  
Director of GIAC. GSEC and PMP certified  
B.S., Engineering, Rochester Institute of Technology

Jess Garcia  
M.S., Faculty, SANS Certified Instructor.  
M.S., Univ. Politecnica de Madrid

David Hoelzer  
B.S., Certified Instructor, Fellow.  
Most Advanced Degree in Information Technology, Summa Cum Laude

Rob Lee  
M.B.A., Faculty, SANS Fellow.  
B.S., Space Operations Engineering, U.S. Air Force Academy,  
M.B.A., Georgetown University

Randy Marchany  
M.S., Faculty, SANS Certified Instructor.  
B.S., Virginia Polytechnic and State University, M.S., ibid.

Stephen Northcutt  
B.S., President, Ex-Officio Director on the Board of SANS Technology Institute, Faculty, SANS Fellow.  
B.S., Mary Washington College

Alan Paller  
M.E., Chair and Director on Board of SANS Technology Institute, Faculty.  
M.E, Massachusetts Institute of Technology, B.S., Cornell University

Megan Restuccia  
M.B.A., Faculty, SANS Certified Instructor.  
M.B.A. Colombia University, B.S., William Paterson University

Marcus Sachs  
M.S., Faculty, SANS Fellow.  
M.S., James Madison University and University of Texas at Austin

Richard Salgado  
J.D., Faculty, SANS Senior Instructor.  
J.D., Law, Yale University

Eugene Schultz  
Ph.D., Faculty, SANS Certified Instructor.  
Ph.D. Purdue University

Dave Shackleford  
M.B.A., Director on the Board of SANS Technology Institute, Faculty, SANS Certified Instructor.  
M.B.A., Georgia State University

Ed Skoudis  
M.S., Director on the Board of SANS Technology Institute, Faculty, SANS Fellow.  
M.S., Carnegie Mellon University, B.S., University of Michigan

Raul Siles  
M.S., Faculty, SANS Certified Instructor.  
M.S., Universidad Politécnica de Madrid

John Strand  
M.S., Faculty, SANS Certified Instructor.  
M.S., University of Denver

Johannes Ullrich  
Ph.D., Dean of Faculty, Chief Research Officer.  
Ph.D., SUNY

Benjamin Wright  
J.D., Faculty, SANS Senior Instructor.  
J.D., Law, Georgetown University Law Center

Lenny Zeltser  
M.B.A., Director on the Board of SANS Technology Institute, Faculty, SANS Senior Instructor.  
M.B.A., M.I.T.
I. All Applicants Complete this Section:

Name ____________________________________________________________

Street Address ______________________________________________________

City ___________________________ State ___________ Zip Code __________

County ___________________________ Country ____________________________

E-mail Address (the best one to reach you) ________________________________

Employer ____________________________________________________________

Position/Title __________________________________________ # of years employed there __________

Phone Number ___________________________________________ Is it Home or Wk # ☐ Home ☐ Work

(with country code if applicable)

Date of Birth _________________________________________________________

Have you previously applied for admission to SANS Technology Institute? ☐ Yes ☐ No

How did you hear about STI’s Master’s Programs? ________________________________

GIAC Gold: If applicable, list your current GIAC Gold Certification(s) [and the related exam score(s) and expiration date(s) if you have them available]:

___________________________________________________________________________

GIAC Certifications: If applicable, list your current GIAC Certs [and the related exam score(s) and the issue date(s) and expiration date(s) if you have them available]:

___________________________________________________________________________

Select a Program of Study:

☐ Masters of Science in Information Security Management

☐ Masters of Science in Information Security Engineering

College or University (Degree - Major - Completion Date - GPA):

___________________________________________________________________________

Request your college to mail your transcript DIRECTLY to SANS Technology Institute

Person to be notified in case of an emergency (Name, Relationship, Address, E-mail, Phone):

___________________________________________________________________________

Gender (Optional - for statistical purposes only):

☐ Male ☐ Female

Ethnic Origin (Optional - for statistical purposes only):

☐ Black ☐ American Indian or Alaskan Native ☐ Asian or Pacific Islander ☐ Hispanic

☐ White ☐ Foreign ☐ Other __________________________
**First Essay** - Over-All Outcome Statement:
*The quality of your writing (content, spelling, grammar, etc.) is important.*

One sentence up to a maximum of two typed pages – single spaced, with double space between paragraphs. Please submit it with your application. Describe what you reasonably expect to achieve by earning a master’s degree from SANS Technology Institute. Some examples are provided below:

- I want to become a college instructor.
- I also want to become a SANS instructor.
- I want to become a senior policy maker in government.
- I want this program to help me develop the skills and knowledge to become a CISO (Chief Information Security Officer) at a Fortune 500 company.

Format for First Essay:
Applicant’s Name: ____________________________
Date: ____________________________

Summary of What I Expect to Achieve by Earning my Master’s Degree: [Applicant must list at least one goal; many applicants list several goals]

Background: [Provide background information/details about the above goal(s)]

**Second Essay** - Leadership:
*The quality of your writing (content, spelling, grammar, etc.) is important.*

Two to three typed pages – single spaced, with double space between paragraphs. Please submit it with your application. Read the following instructions and then write an essay describing leadership qualities which you have demonstrated in the past. We define “leadership” and leadership “competencies” in the Leadership Essay article by President Stephen Northcutt at www.sans.edu/resources/leadershiplab.

**Part A:** In Part A of your essay, list three competencies that you believe you have some strength in and provide examples. It is perfectly acceptable to refer to a competency that is not listed in that article.

**Part B:** Start Part B of your essay on a SEPARATE page. Please list three competencies that you want to work on.

**NOTE about the Leadership Essay:** If you are accepted into the master’s program of SANS Technology Institute (STI), you hereby give permission to STI to post Part A of your Leadership Essay on-line on the STI website or at STI’s Leadership Laboratory at www.sans.edu/resources/leadershiplab. STI will not be required to post it, but STI will have the choice. We understand that some information may be sensitive. As one example, sometimes applicants do not want to name a particular place, time, or company in their essay. We have no objection to your use of a fictitious place, time, or company name in your essay. However, your own name, as the author of the Leadership Essay, must be on your essay.

**II. Applicants residing outside the United States must complete this section:**

Country of Citizenship
If you are a resident alien, please enclose a copy of your appropriate documentation with your application. If English is not your native language you need to provide evidence of the appropriate TOEFL score [or a Certificate of Proficiency in English (CPE) at level 5 in the Cambridge five level systems]. Keep in mind that you are applying for a program that is intensive in English language writing, speaking, and presenting.

- ☐ Yes  ☐ No  Date of Exam ____________________________________________  TOEFL Score ____________________________________________

List close relatives or friends in the United States:

<table>
<thead>
<tr>
<th>Name</th>
<th>Relationship</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Relationship</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Address</th>
<th>E-mail</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

III. All Applicants Complete this Section

ALL APPLICATION MATERIALS BECOME A PART OF THE PERMANENT RECORDS OF THE SANS TECHNOLOGY INSTITUTE AND ARE NOT RETURNED. It is your responsibility to be sure your application materials (including your application fee) are complete and have all been received by the SANS Technology Institute.

In complying with the letter and spirit of applicable laws and in pursuing its own goals of pluralism, SANS Technology Institute shall not discriminate on the grounds of race, color, religion, sex, sexual orientation, national origin or citizenship status, age, disability, or Veterans status in employment and education.

I understand that SANS Technology Institute (STI) uses the services of STI's affiliate, SANS, for some of the training; and STI uses the services of STI’s affiliate, GIAC, for some of the assessment. By submitting to STI this application for admission, I am authorizing SANS to release my training dates/locations and related information to STI, and I am authorizing GIAC to release my exam/paper scores and related information to STI. This information can be used by STI in the application review process, academic advising, transcript maintenance, progress tracking, and other educational purposes. Also, by submitting this application, I acknowledge that I understand and accept the GIAC tradition of posting all persons' names and GIAC exam scores that are considered passing by GIAC onto the GIAC Web site.

Signature: ____________________________  Date: ____________________________
EMPLOYER ENDORSEMENT FOR SANS TECHNOLOGY INSTITUTE’S COHORT 2013

STI’s accelerated cohort master’s programs will require a student to be away from the office a significant amount of time during the 26 month program: about 33 days of attending class and a large amount of time outside the classroom will also be required for the student’s success. The learning experience will enable students to use their new skills and knowledge immediately and the student will continue to build on these strengths throughout the program. Employer endorsement of the student is required before the student will be admitted into the program. Below is a chart of approximate time requirements for both STI master’s programs. However, each person is unique so many of the numbers may vary depending on individual circumstances. NOTE: The admission and curriculum requirements in effect when a person is admitted to STI are the requirements that will apply to that person.

Master of Science in Information Security Management (MSISM)

Course Time:

<table>
<thead>
<tr>
<th>Course</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGT305: Technical Communications &amp; Presentation Skills for Security Professionals</td>
</tr>
<tr>
<td>MGT512: SANS Security Leadership Essentials For Managers with Knowledge Compression™</td>
</tr>
<tr>
<td>SEC504: Hacker Techniques, Exploits, and Incident Handling</td>
</tr>
<tr>
<td>MGT438: How to Establish a Sec Awareness Program (Course may be lengthened)</td>
</tr>
<tr>
<td>MGT404: Fundamentals of Info Sec Policy (Course may be lengthened)</td>
</tr>
<tr>
<td>MGT421: SANS Leadership and Management Competencies</td>
</tr>
<tr>
<td>AUD507 Auditing Networks, Perimeters, and Systems</td>
</tr>
<tr>
<td>MGT525: Project Management and Effective Communications for Security Professionals and Managers</td>
</tr>
<tr>
<td>LEG523: Law of Data Security and Investigations</td>
</tr>
<tr>
<td>MGT411: SANS 27000 Implementation and Management</td>
</tr>
<tr>
<td>Total Class Time</td>
</tr>
</tbody>
</table>

Additional time is described below for study/preparation for exams, gold papers/written assignments, community project requirements, etc.

Exams (Approximate Study Time)
Students must pass each exam with an 80 or higher. Approximate study times for GIAC exams range from 40 to 85 hours out-side of the classroom for each exam. Times will vary depending on each student’s experience. Most exams must be completed in 4 hours, some exams are 2 hours.

Written Assignments and Gold Papers (Approximate Preparation Time)
The MSISM program requires seven GIAC Gold papers. Approximate preparation and research time for each paper is estimated to be between 20 and up to more than 80 hours depending on the student’s topic and number of research issues. When a Gold Paper is not available, the college provides Written Assignments. There are about three Written Assignments for a total of approximately 30 hours.

Community Project Requirements (See on next page)

Master of Science in Information Security Engineering (MSISE)

Course Time:

<table>
<thead>
<tr>
<th>Course</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGT305: Technical Communications &amp; Presentation Skills for Security Professionals</td>
</tr>
<tr>
<td>SEC401: SANS Security Essentials Bootcamp Style</td>
</tr>
<tr>
<td>SEC503: Intrusion Detection In-Depth</td>
</tr>
<tr>
<td>SEC504: Hacker Techniques, Exploits, and Incident Handling</td>
</tr>
<tr>
<td>MGT438: How to Establish a Security Awareness Program (Course may be lengthened)</td>
</tr>
<tr>
<td>MGT404: Fundamentals of Information Security Policy (Course may be lengthened)</td>
</tr>
<tr>
<td>MGT421: SANS Leadership and Management Competencies</td>
</tr>
<tr>
<td>MGT525: Project Management and Effective Communications for Security Professionals and Managers</td>
</tr>
<tr>
<td>FOR508: Advanced Computer Forensic Analysis and Incident Response OR Software Security Training</td>
</tr>
<tr>
<td>Two Electives</td>
</tr>
<tr>
<td>Total Class Time</td>
</tr>
</tbody>
</table>


Additional time is described below for study/preparation time for exams, gold papers/written assignments, community project requirements, etc.

**Exams (Approximate Study Time)**
Students must pass each exam with an 80 or higher. Approximate study times for GIAC exams range from 40 to 85 hours outside of the classroom for each exam. Times will vary depending on each student's experience. Most exams must be completed in 4 hours, some exams are 2 hours.

**Written Assignments and Gold Papers (Approximate Preparation Time)**
The MSISE program requires five GIAC Gold papers. Approximate preparation and research time for each paper is estimated to be between 20 hours and up to more than 80 hours depending on the student's topic and number of research issues. When a Gold Paper is not available, the college provides Written Assignments. There are about three Written Assignments for a total of approximately 30 hours.

**Community Project Requirements (Approximate Preparation Time)**
Both the MSISM and MSISE programs have seven Community Project Requirements. Below is a list of the projects and approximate preparation times:

- Work Study for one of the courses above. Course time incorporated in chart above. Set up/tear down requires additional time, so it results in a total of about seven days. An essay also is required.
- Group Discussion and Written Project – 24 hours from time of assignment to delivery
- Joint Written Project – 20 hours
- First Presentation – 10 hours
- Second Presentation – 10 hours
- Teaching Assistant (MSISM only) – 6 days (possibly some evenings)
- GSE (MSISE only) – 49 hours
  - Two days of labs – 16 hours
  - Multiple choice qualifying exam – up to 3 hours
  - Study/preparation time for GSE – 30 hours
- Security Awareness Talk – 20 hours
(Reflections papers are required for some of the above – 8 hours)

I endorse the participation of ________________________________ in the STI Cohort master's program and acknowledge that I have read and understand the approximate time requirements for this program.

Organization: ________________________________________________________________________________________________

Approving Manager's Name (print): ____________________________________________________________________________

Approving Manager’s Title: __________________________________________________________________________________

Approving Manager’s Signature: ______________________________________________________________________________

Relationship to Applicant: _____________________________________________________________________________________

Date: ______________________________________________________________________________________________________

Please complete the information and return to:
SANS Technology Institute
8120 Woodmont Ave. Ste. 205
Bethesda, Maryland 20814
STUDENT DECLARATION FOR SANS TECHNOLOGY INSTITUTE’S COHORT 2013

STI’s accelerated cohort master’s options will require you to be away from the office a significant amount of time during the twenty-six month program: about 33 days of attending class and a large amount of time outside the classroom will also be required for your success. The learning experience will enable you to use your new skills and knowledge immediately and you will continue to build on these strengths throughout the program. This form shows approximate times for each aspect of the master’s program and was designed to help you with scheduling your time. However, each person is unique so many of the numbers may vary depending on individual circumstances. Below is a chart of approximate time requirements for both STI master’s programs. NOTE: The admission and curriculum requirements in effect when a person is admitted to STI are the requirements that will apply to that person.

Master of Science in Information Security Management (MSISM)

Course Time:

<table>
<thead>
<tr>
<th>Course</th>
<th>Days</th>
<th>Total Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGT305: Technical Communications &amp; Presentation Skills for Security Professionals</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>MGT512: SANS Security Leadership Essentials For Managers with Knowledge Compression™</td>
<td>5</td>
<td>43</td>
</tr>
<tr>
<td>SEC504: Hacker Techniques, Exploits, and Incident Handling</td>
<td>6</td>
<td>48</td>
</tr>
<tr>
<td>MGT438: How to Establish a Sec Awareness Program (Course may be lengthened)</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>MGT404: Fundamentals of Information Security Policy (Course may be lengthened)</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>MGT421: SANS Leadership and Management Competencies</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>AUD507 Auditing Networks, Perimeters, and Systems</td>
<td>6</td>
<td>48</td>
</tr>
<tr>
<td>MGT525: Project Management and Effective Communications for Security Professionals and Managers</td>
<td>6</td>
<td>48</td>
</tr>
<tr>
<td>LEG523: Law of Data Security and Investigations</td>
<td>5</td>
<td>40</td>
</tr>
<tr>
<td>MGT411: SANS 27000 Implementation and Management</td>
<td>1</td>
<td>8</td>
</tr>
</tbody>
</table>

Total Class Time 33 days 264

Additional time is described below for study/preparation for exams, gold papers/written assignments, community project requirements, etc.

Exams (Approximate Study Time)

Students must pass each exam with an 80 or higher. Approximate study times for GIAC exams range from 40 to 85 hours outside of the classroom for each exam. Times will vary depending on each student’s experience. Most exams must be completed in 4 hours, some exams are 2 hours.

Written Assignments and Gold Papers (Approximate Preparation Time)

The MSISM program requires seven GIAC Gold papers. Approximate preparation and research time for each paper is estimated to be between 20 and up to more than 80 hours depending on the student’s topic and number of research issues. When a Gold Paper is not available, the college provides Written Assignments. There are about three Written Assignments for a total of approximately 30 hours.

Community Project Requirements (See on next page)

Master of Science in Information Security Engineering (MSISE)

Course Time:

<table>
<thead>
<tr>
<th>Course</th>
<th>Days</th>
<th>Total Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGT305: Technical Communications &amp; Presentation Skills for Security Professionals</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>SEC401: SANS Security Essentials Bootcamp Style</td>
<td>6 + 5 evenings</td>
<td>52</td>
</tr>
<tr>
<td>SEC503: Intrusion Detection In-Depth</td>
<td>6</td>
<td>48</td>
</tr>
<tr>
<td>SEC504: Hacker Techniques, Exploits, and Incident Handling</td>
<td>6</td>
<td>48</td>
</tr>
<tr>
<td>MGT438: How to Establish a Security Awareness Program (Course may be lengthened)</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>MGT404: Fundamentals of Information Security Policy (Course may be lengthened)</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>MGT421: SANS Leadership and Management Competencies</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>MGT525: Project Management and Effective Communications for Security Professionals and Managers</td>
<td>6</td>
<td>48</td>
</tr>
<tr>
<td>FOR508: Advanced Computer Forensic Analysis and Incident Response OR Software Security Training</td>
<td>6</td>
<td>48</td>
</tr>
<tr>
<td>Two Electives</td>
<td>12</td>
<td>96</td>
</tr>
</tbody>
</table>

Total Class Time 33 days + 5 eves 372
STUDENT DECLARATION FOR SANS TECHNOLOGY INSTITUTE’S COHORT 2013

Additional time is described below for study/preparation time for exams, gold papers/written assignments, community project requirements, etc.

Exams (Approximate Study Time)
Students must pass each exam with an 80 or higher. Approximate study times for GIAC exams range from 40 to 85 hours outside of the classroom for each exam. Times will vary depending on each student’s experience. Most exams must be completed in 4 hours, some exams are 2 hours.

Written Assignments and Gold Papers (Approximate Preparation Time)
The MSISE program requires five GIAC Gold papers. Approximate preparation and research time for each paper is estimated to be between 20 hours and up to more than 80 hours depending on the student’s topic and number of research issues. When a Gold Paper is not available, the college provides Written Assignments. There are about three Written Assignments for a total of approximately 30 hours.

Community Project Requirements (Approximate Preparation Time)
Both the MSISM and MSISE programs have seven Community Project Requirements. Below is a list of the projects and approximate preparation times:

• Work Study for one of the courses above. Course time incorporated in chart above. Set up/tear down requires additional time, so it results in a total of about seven days. An essay also is required.
• Group Discussion and Written Project –24 hours from time of assignment to delivery
• Joint Written Project – 20 hours
• First Presentation – 10 hours
• Second Presentation – 10 hours
• Teaching Assistant (MSISM only) – 6 days (possibly some evenings)
• GSE (MSISE only) – 49 hours
  - Two days of labs – 16 hours
  - Multiple choice qualifying exam – up to 3 hours
  - Study/preparation time for GSE – 30 hours
• Security Awareness Talk – 20 hours

(Reflections papers are required for some of the above – 8 hours)

I have read and understand the approximate time requirements for the STI Cohort 2013 master’s program.

Applicant’s Name: ____________________________________________________________

Applicant’s Signature: _______________________________________________________

Date: ___________________________________________________________________

Please complete the information and return to:
SANS Technology Institute
8120 Woodmont Ave.  Ste. 205
Bethesda, Maryland  20814
The mission of SANS is to foster original research in information security using a community-oriented, consensus approach, codify the results of that work into high-quality educational material, and then teach the knowledge with excellence.

A certification is proof an individual meets a minimum standard. The mission of GIAC is to provide assurance to employers their people and prospective hires can actually do the job. To accomplish this mission, GIAC goes beyond theory and terminology and tests the pragmatics of Audit, Security, Operations, Management and Software Security tasks.

The mission of STI is to develop the information security technology leaders needed to help strengthen the information community all over the world by improving the security of cyberspace. STI seeks to prepare both the managers of information security groups and the technical leaders who direct security technology programs. STI’s primary functional emphasis is instruction, but the Institute’s faculty and students will engage in research and public service programs.