



 **Software Engineering Institute**

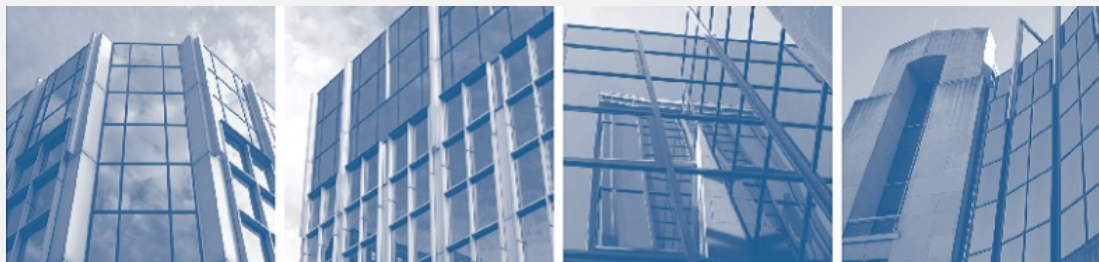
CERT-Certified Computer Security Incident Handler (CSIH) Certification Guidebook

Revised 20 Jan 2012

The Software Engineering Institute (SEI) is a federally funded research and development center sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University.

This material is approved for public release.

© 2012 by Carnegie Mellon University



CarnegieMellon

Copyright 2012 Carnegie Mellon University.

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this report is not intended in any way to infringe on the rights of the trademark holder.

Internal use. Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

External use. This document may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about SEI publications, please visit the library on the SEI website (www.sei.cmu.edu/library).

The CERT-Certified CSIH Certification is administered by

Software Engineering Institute
Carnegie Mellon University
Professional Certification Program
4500 Fifth Avenue
Pittsburgh, PA 15213-2612 USA

Phone +1.412.268.5800
Toll free +1.888.201.4479
Fax +1.412.268.5857

Email: certification-info@sei.cmu.edu

Table of Contents

| | |
|--|-----------|
| Introduction | 5 |
| What is Professional Certification? | 5 |
| What are the Advantages of Obtaining Professional Certification? | 5 |
| Who Should Obtain CSIH Certification? | 6 |
| Why Obtain CSIH Certification? | 6 |
| SEI Certification Standards | 6 |
| Applicant Eligibility Requirements | 7 |
| General Policy Regarding Applicants and Application Evaluations | 7 |
| How to Apply for CSIH Certification | 8 |
| The CSIH Certification Process | 8 |
| Completing the Certification Application | 8 |
| Submitting the Certification Application | 9 |
| Notification of Application Status | 9 |
| Incomplete Applications | 10 |
| Application Acceptance | 10 |
| Application Rejection | 10 |
| Application Rejection Appeals Process | 11 |
| Scheduling and Preparing for the Exam | 12 |
| Test Center Locations | 12 |
| On-Line Test Registration | 12 |
| Special Accommodation Requests | 13 |
| Changing or Canceling a Scheduled Exam | 15 |
| No-Show Candidates | 15 |
| The CSIH Examination | 16 |
| Examination Overview | 16 |
| Preparation for the Exam | 16 |
| Exam Content Areas | 16 |
| Taking the Certification Exam | 20 |
| Test Center Rules | 20 |
| After the Certification Exam | 21 |
| The Exam Score | 21 |
| How the Passing Score was Set | 21 |
| Notification of Results | 22 |
| Certificates | 22 |
| Retaking the Exam | 22 |

| | |
|---|-----------|
| Recertification | 23 |
| Recertification Requirements..... | 23 |
| Professional Development Units (PDUs) | 23 |
| Record Keeping and Documentation | 25 |
| Rejected Renewal Activity Log Entries | 25 |
| SEI Audit of the CSIH Certification Renewal Program | 26 |
| | |
| SEI Certification Program Policies..... | 27 |
| Policy on the Code of Professional Conduct..... | 27 |
| Policy on Ethics..... | 27 |
| Policy on Governance..... | 27 |
| Policy on Conflict of Interest | 27 |
| Policy on Confidentiality, and Privacy Statement for Data Collected..... | 27 |
| Policy on Certification Documentation and Materials | 28 |
| Policy on the Family Educational Rights and Privacy Act (FERPA)..... | 28 |
| Policy on Logos, Service Marks, and Trademarks..... | 28 |
| Policy on Examination Irregularities..... | 28 |
| Policy on Examination Score Validity | 29 |
| Policy on Requests for Examination Rescoring..... | 30 |
| Policy on Appeals of Adverse Decisions | 30 |
| | |
| Revocation, Suspension, Expiration, or Surrender of Certification..... | 32 |
| Revocation of Certification..... | 32 |
| Suspension of Certification..... | 32 |
| Reinstatement of Certification after Suspension | 33 |
| Expiration of Certification | 33 |
| Resignation and Voluntary Surrender of Certification | 33 |
| Appeals of Decisions to Revoke or Suspend Certification | 34 |
| | |
| Appendix A: Completion Guidelines for CSIH Application Form..... | 35 |
| Appendix B: CSIH Application Form/SEI Certification Agreement | 38 |
| Appendix C: CSIH Recommendation Letter Submission Form | 45 |
| Appendix D: SEI Code of Professional Conduct Commitment Form..... | 49 |

Introduction

This guidebook contains information on how to apply for the CERT Computer Security Incident Handler (CSIH) Certification.

The CSIH Certification is maintained and granted by the Software Engineering Institute (SEI), a federally funded research and development center (FFRDC) operated by Carnegie Mellon University (CMU). The SEI performs a variety of operations that includes the identification, development, and advocacy of practices for developing, acquiring, delivering, and maintaining high-quality software products and services, and for protecting networked systems. In furtherance of its mission to transition technology into widespread practice, the SEI grants certification to individuals who demonstrate proficiency in the skills, abilities, and knowledge pertaining to specific technology areas.

Certification applicants are encouraged to read the entire guidebook carefully before beginning the application process to ensure that they meet all of the eligibility requirements for becoming a CERT-Certified Computer Security Incident Handler.

What is Professional Certification?

Professional certification is a mechanism by which professionals can demonstrate their mastery of the essential core skills, knowledge, and principles relevant to a particular professional field. Certifications differ from certificate programs in that certifications generally include requirements for competency and skill in the field and for passing a proficiency examination to ensure that an individual meets the entry standards established by the certifying body. By contrast, certificates are usually awarded at the completion of a course or a program of study, and the award of the certificate does not require the recipient to meet examination performance standards or experience requirements.

What are the Advantages of Obtaining Professional Certification?

Certification provides employers and consumers with an assurance that the certified individual has attained a well-defined level of understanding or ability against a particular skill set or body of knowledge, and has maintained that level of expertise over a specific period of time. The requirement for renewal of certification ensures that certified individuals continually maintain and expand their knowledge and skills in the profession while keeping abreast of advancements and updates in their field. Certification is required for employment in some professions, whereas in other fields, certification provides a competitive advantage to individuals who hold a particular credential.

Who Should Obtain CSIH Certification?

The CERT-Certified Computer Security Incident Handler (CSIH) certification program has been created for

- computer network incident handling and incident responder professionals
- computer security incident response team (CSIRT) members and technical staff
- system and network administrators with incident handling experience
- incident handling educators
- cyber security technical staff

The CSIH certification is recommended for computer security professionals with one (1) or more years of experience in incident handling and/or equivalent security-related experience.

The CSIH certification program supports those individuals who are computer incident handling or incident responder professionals, computer security incident response team (CSIRT) members, network security technical staff, and other information assurance practitioners who are involved in incident handling functions. More specifically, CERT-Certified Computer Security Incident Handlers

- are knowledgeable and skilled in the latest practices in the cyber security field
- have the abilities and skills to help an organization reach its security goals
- have completed an industry-leading qualification track
- are committed to a professional code of conduct that separates them from all other practitioners in the field
- ensure that their organizations stay current on recent innovations and research in the computer security field

Why Obtain CSIH Certification?

Every organization relies on professionals who are highly skilled in various security practices to operate successfully in today's cyber environment. These same organizations have discovered that using certifications is an effective way to identify, hire, and promote motivated and skilled individuals in the organization.

Recently, the United States Department of Defense (US DoD) passed Directive 8570.1M, which mandates that all DoD Information Assurance personnel must obtain and maintain a security certification pertinent to their job requirements.

SEI Certification Standards

Certification foundations for competency and skill, as well as credentialing operations, will be compliant with ANSI/IEC/ISO 17024 standards. ANSI/IEC/ISO 17024 sets an

internationally-recognized benchmark to assure that the certification organization meets set standards. It assures that the certifying organization operates in a consistent, comparable, and reliable manner. It also provides an independent third party review process that leads to accreditation for the certification program.

Applicant Eligibility Requirements

Applicants must comply with all policies, procedures, and requirements of the CSIH Advisory Board that are in effect at the time the application is filed. These requirements include

- professional experience of at least one year in computer security incident management activities
- recommendation of the applicant's current employer/manager
- successful completion of the application screening and examination processes

General Policy Regarding Applicants and Application Evaluations

All applications are evaluated without regard to the applicant's age, gender, race, ancestry, national origin, religion, creed, marital status, sexual orientation, or disability, in accordance with Carnegie Mellon University's Statement of Assurance.

This Statement of Assurance applies to all departments and programs of CMU, including CERT and the SEI, and states that Carnegie Mellon University may not discriminate in admission, employment, or administration of its programs on the basis of religion, creed, ancestry, belief, age, veteran status, sexual orientation, or gender identity. Carnegie Mellon does not discriminate in violation of federal, state, or local laws or executive orders.

Carnegie Mellon University does not discriminate and Carnegie Mellon University is required not to discriminate in admission, employment, or administration of its programs or activities on the basis of race, color, national origin, sex, or handicap in violation of Title VI of the Civil Rights Act of 1964, Title IX of the Educational Amendments of 1972, and Section 504 of the Rehabilitation Act of 1973, or any other federal, state, or local laws or executive orders.

For more information, see www.cmu.edu/policies/documents/SoA.html.

How to Apply for CSIH Certification

The CSIH Certification Process

To receive the CERT CSIH Certification, an applicant must complete all of the following required steps.

1. Submit a signed copy of the certification application along with evidence of one (1) or more years of experience in incident handling in a technical and/or management role. Incident handling experience must have been obtained within seven (7) years of submission of the certification application. A detailed résumé or curriculum vitae listing relevant experience should be included with the application. The application and all supporting forms (listed in Steps 2, 3, and 4 below) are included in Appendix A of this guidebook and online at www.sei.cmu.edu/certification/security/csih.
2. Submit a completed Certification Recommendation Form signed by the applicant's current manager.
3. Agree (by signature on the document) to abide by the SEI Code of Professional Conduct.
4. Agree (by signature on the certification application) to abide by the SEI Certification Policies and Procedures.
5. Receive written confirmation from the SEI of candidacy acceptance. SEI Certification personnel will review the application and associated documentation for completeness and conformance to the experience standards required by the program. (Applicants who are not accepted will receive written notification that includes information regarding areas that need to be improved or remediated.)
6. Register for and complete the CSIH written exam. The fee for the examination is \$499 (USD).
7. Earn a passing score on the CSIH exam. Successful candidates will receive a welcome kit that contains the certification documentation, certificate, and other information relevant to SEI certificate holders.

Completing the Certification Application

Applicants may apply for the exam using either the paper form located in Appendix B of this guidebook or a downloaded form from the SEI Certification website found at www.sei.cmu.edu/certification/security/csih. Instructions and guidelines for completing the forms can be found in Appendix A of this guidebook.

Submitting the Certification Application

All applicants must sign an affirmation attesting that the information submitted on the application is complete and true. For applications submitted by fax or postal service delivery, an actual signature on the paper copy of the form is required. For applications submitted by email, a scanned signature on paper copy or an electronic signature is permissible.

Applicants should provide their managers with a copy of the recommendation form to be completed and placed in a sealed envelope by the manager, along with the manager's business card. The manager should sign across the seal, and may either return the recommendation to the applicant or submit the recommendation directly to the SEI at the postal service delivery address shown below.

Applicants should retain a copy of the application and supporting materials for the duration of the application process. Applicants may use one of the following methods for submitting the completed application package.

- Fax the completed application and supporting documents (except sealed recommendation form) to the attention of the SEI Certification Program. The fax number is +1.412.268.5758. Please remit the sealed recommendation form by regular postal service.
- Email a scanned or digitally signed application with supporting documents (except sealed recommendation form) to certification-info@sei.cmu.edu. Please remit the sealed recommendation form by regular postal service.
- Mail the application and all supporting documents (including sealed recommendation form) via postal service or document carrier to the address below:

Software Engineering Institute
Carnegie Mellon University
Attn: CSIH Certification Program Manager / J. Welch
4500 Fifth Avenue
Pittsburgh, PA 15213

Notification of Application Status

Applicants will be notified as to their application status approximately two (2) to six (6) weeks after the application has been received and processed by SEI Certification Program personnel.

Eligible applicants will be notified of the acceptance of their application, after which the candidate has twelve (12) months to complete the exam. The SEI Certification Program Manager will contact successful applicants to make arrangements for the certification examination.

The twelve-month window begins when the application approval email is sent from the SEI. If the candidate is unable to complete the examination within that timeframe, the SEI will refund the examination fee upon written request from the candidate, as long as the request for refund is received prior to the end of the application validity period. If the application process is not completed within the allotted one-year window, the candidate must submit a new application package, including the \$499 (USD) examination fee.

Ineligible applicants will be notified by the SEI Certification Program Manager as to the reason(s) that their application was not acceptable, and will be provided with information identifying the gaps or problems with the application documentation. The applicant will be given the option either to correct and resubmit the application or to withdraw the application and request a refund of the examination fee.

Incomplete Applications

Incomplete applications will be returned to the applicant. Applicants who submit an incomplete application will receive an email from the CSIH Certification Program Manager indicating the materials or information needed to make the application complete.

Application Acceptance

Successful applicants will receive notification of acceptance from the SEI Certification Program Manager, who will assist in arranging the certification exam. Candidates have twelve (12) months from the date of acceptance to complete the certification exam.

Application Rejection

- Applications for certification may be rejected for any of the following reasons.
- Falsification of work experience or of other information on the examination application
 - Misrepresentation of work experience or of other information on the examination application
 - Incomplete application package
 - Violation of testing procedures
 - Failure to pass the certification examination

Individuals whose applications are rejected may follow the appeals process outlined on page 11 of this guidebook. Please note that there is no appeals process for applicants who do not meet the minimum employment requirements or have submitted an incomplete application package. Applicants who are found to be

ineligible because they do not meet the minimum eligibility requirements will receive a refund of the exam application fee. Applicants whose recommendation request form did not meet the necessary requirements will be notified by the SEI Certification Program Manager.

Application Rejection Appeals Process

Individuals whose applications are rejected for any of the above-stated reasons will be notified in writing. Applicants may appeal the decision to the CSIH Certification Program by using the appeals procedure delineated below.

1. All appeals must be presented in writing to the CSIH Advisory Board Chair, 4500 Fifth Avenue, Suite 2300A, Pittsburgh, PA 15213.
2. The appeal must contain all information and/or documentation in support of the claim that the CSIH certification program's decision to reject admissions credentials, or eligibility status was erroneous.
3. A non-refundable processing fee of \$150 must accompany the written request for appeal.
4. The written request for appeal must be postmarked within thirty (30) calendar days of the date on the notification from the CSIH certification program denying the application.
5. The appeal and supporting documentation must be sent to the CSIH Advisory Board Chair by certified mail.
6. The relevant appeals subcommittee will review the petition and conduct a hearing to decide on the petition. The appellant is invited to attend to support the petition.
7. The relevant appeals subcommittee will render a decision and inform the appellant and SEI Certification.
8. The appeals subcommittee will act on the appeal within sixty (60) calendar days after the receipt of the appellant's written notification and supporting documentation. The decision of the appeals subcommittee will be final and binding on the appellant and the CSIH certification program.
9. The CSIH Advisory Board Chair will send a written summary of the appeals subcommittee's decision to the appellant by certified or registered mail within ten (10) business days of receiving the appeals subcommittee's ruling.
10. Should the appellant further challenge the decision, the issue may be scheduled for consideration by the full CSIH Advisory Board at their next scheduled meeting. (Note: Only board members who were not involved in the previous review will be allowed to vote on this appeal.)

An appeal will be considered closed and all proceeding ended when either of the following occurs.

1. An appeal has been resolved and the appellant has been notified in writing of the decision.
2. The appeal has been withdrawn or terminated by the appellant.

If the CSIH Certification Program revokes a certificant's credential, the certificant shall immediately surrender his/her certificate and copies thereof to the CSIH Advisory Board Chair upon receipt of the notice or revocation.

Scheduling and Preparing for the Exam

Successful applicants will receive notification of acceptance from the SEI Certification Program Manager, who will assist in arranging the certification exam. Candidates have twelve (12) months from the date of application acceptance to complete the exam.

Test Center Locations

The CSIH examination can be taken at one of the SEI's USA offices (Pittsburgh, PA or Arlington, VA), at the SEI Europe office (Frankfurt, Germany), or at one of the testing network locations listed on the Kryterion website (www.kryteriononline.com). The examination is sometimes offered at selected conferences and SEI events; such opportunities will be advertised in the "Certification News" section on the SEI Certification website (www.sei.cmu.edu/certification).

On-line Test Registration

Candidates may register for the exam online by following the steps listed below.

1. Access the SEI's testing services portal using the following URL:
<https://www.webassessor.com/was.do?page=publicHome&branding=SEI>
2. Create a personal account and follow the instructions for new users of the testing system.
3. Log on to the registration page and click the button called "Register for Exam" (located at the top of the page on the right-hand side).
4. On the "Exam Registration" page, click "Buy Now" next to "CERT Computer Security Incident Handler Examination." Note: clicking "Buy Now" does not require completion at this time of the purchase of the exam.
5. On the "Select Testing Center" page, use the drop-down menus at the top of the page to tailor the search for a testing center by country, state, zip code, etc.
6. On the "Date and Time Selection" page, schedule a testing session by selecting a date and starting time. After scheduling the test session and acknowledging having read the "no-shows and cancellations" policy, click the blue "Select" button. On the "Shopping Cart" page, if everything appears to be correct, click the blue "Check Out" button.
7. On the "Checkout" page, provide the appropriate billing and payment information, and click the blue "Submit" button. When the "Submit" button is clicked, the credit card charge will be processed.
8. After the exam has been purchased, the Kryterion system will send an email that confirms the purchase and provides important information about the testing session, including a candidate authorization code. Please print out the confirmation email, as the candidate authorization code is required in order for the proctor to launch the exam at the test center.

Special Accommodation Requests

It is SEI policy to provide candidates with disabilities with a fair and equal opportunity to demonstrate their knowledge and skill in the essential functions being measured by SEI certification examinations. All reasonable requests for special accommodation will be fulfilled to the maximum extent possible, provided that the SEI Certification Program offices receive such requests in writing at least thirty (30) calendar days in advance of the candidate's scheduled examination.

Reasonable accommodations are decided by the SEI Certification Program Manager on a case-by-case basis, based upon the individual's specific request, specific disability, submitted documentation, and appropriateness of the request. Reasonable accommodations do not include actions that fundamentally alter the purpose or nature of the examination. Reasonable accommodations generally are provided for candidates who

- have a physical or mental impairment that substantially limits that person in one or more major life activities (e.g., walking, talking, hearing, or performing manual tasks)
- have a record of such physical or mental impairment
- are regarded as having a physical or mental impairment

To apply for reasonable special accommodations, candidates must submit a written request and supporting documentation from a licensed health care provider. Documentation must be presented on official letterhead from the health care provider, and must include information that explains the nature of the disability and the specific type of accommodation being requested. The candidate will be informed by email or telephone of the decision to grant or deny the request within five (5) business days following the SEI Certification Program Manager's receipt of the request for special accommodation. This will allow candidates time to change the exam venue or, if necessary, to reschedule or cancel the exam, while remaining in compliance with the requirement for giving 72 hours advance notice for changing or canceling a scheduled exam, as explained on page 15 of this guidebook.

Requests for reasonable special accommodation and supporting documentation may be forwarded to the SEI Certification Program, to arrive no less than thirty (30) calendar days prior to the scheduled examination, by one of the following means:

- Email: certification-info@sei.cmu.edu
- Fax: +1.412.268.5857, attention Certification Program
- Postal Service delivery to:
Software Engineering Institute
Carnegie Mellon University
Attention: Professional Certification Program
4500 Fifth Avenue
Pittsburgh, PA 15213-2612 USA

Please note that Kryterion, the SEI's test delivery vendor, cannot comply with special accommodation requests made by candidates who take the exam outside of the United States, US territories, or Canada, or where local operating conditions or local laws and customs render such requests unlawful, economically unfeasible, or impossible to perform. Incomplete or late requests for special accommodation may not be honored.

Decisions that reject the candidate's request for special accommodation may be appealed in accordance with the SEI's Policy on Appeals of Adverse Decisions, as outlined on page 30 of this guidebook.

Changing or Canceling a Scheduled Exam

Candidates who need to change the date and/or time of their scheduled exam, change the location of the testing center, or cancel the exam must notify the SEI Certification Program offices of the desired change by sending an email to certification-info@sei.cmu.edu at least 72 hours in advance of the scheduled start time of the exam. Changes or cancellations that are requested less than 72 hours in advance of the scheduled test may result in the assessment of a \$150 (USD) fee.

No-Show Candidates

Candidates who do not appear for their scheduled exam appointment, who arrive more than 15 minutes later than the start time of their scheduled appointment, who appear with improper or inadequate identification, or who cancel their examination appointment less than 72 hours prior to the scheduled start time of the exam appointment will be considered no-shows and will forfeit all fees. No-show candidates may reapply for the examination at a future time and may register for another exam upon payment of full fees.

The CSIH Examination

Examination Overview

The development of quality credentialing processes for professionals follows sound and legally defensible procedures based on psychometric examination standards. These standards ensure that the content of the examination is representative of the competence and skills necessary for the particular role being certified. Content validity is the most commonly applied and accepted validation strategy used for establishing certification programs today.

The CSIH exam is designed to demonstrate that cyber security professionals have sufficient knowledge and skills to successfully conduct network security functions in key areas. The exam was developed in accordance with examination development and administration guidelines set forth by the American National Standards Institute standard ISO/IEC/ANSI 17024, the American Educational Research Association, the American Psychological Association (as presented in the 1999 *Standards for Educational and Psychological Testing*), and the National Council on Measurement in Education standards.

The closed-book written examination consists of 65 multiple-choice questions. Each question lists four possible answers, only one of which is the correct or “best possible” answer. The answer to each question can be derived independently of the answer to any other question. Three hours are allotted to complete the exam. The examination currently is available only in English.

Preparation for the Exam

Training is not a requirement for the CSIH certification. Candidates should ensure that they prepare appropriately for questions in the exam content areas listed below.

Exam Content Areas

The CSIH examination tests the candidate with regard to the competency and skills required to successfully perform the role of a Computer Security Incident Handler. The subject matter covered on the certification exam falls into five major weighted content area groupings, as follows.

- Protect Infrastructure (7%)
- Event Incident Detection (17%)
- Triage and Analysis (28%)
- Response (40%)
- Sustainability (8%)

Protect Infrastructure (7%)

- Perform risk assessments in constituent systems
- Assist constituents in correcting problems identified by risk assessment activities
- Identify and gather critical information
- Perform proactive vulnerability scanning on constituent systems and networks
- Assist constituents in correcting problems identified by vulnerability scanning activities
- Assist constituents in correcting problems identified by penetration testing activities
- Conduct operational exercises/incident response exercises (to assess the security posture of the organization)
- Incorporate lessons learned from operational exercises into the constituents' network defenses
- Implement changes to the computing infrastructure (to stop or mitigate an ongoing incident, to stop or mitigate the potential exploitation of a vulnerability, or as a result of postmortem reviews or other process improvement mechanisms)
- Provide constituents with guidance in best practices for protecting their systems and networks

Event Incident Detection (17%)

- Monitor networks and information systems for security
- Analyze the data or indicators from the networks and systems being monitored
- Coordinate with others to validate network alerts
- Construct signatures that can be implemented on monitoring tools (in response to new or observed threats)
- Review and update network and systems configurations or rules sets (in response to changes in the threat environment)
- Monitor external data sources (e.g., vendor sites, security websites) to maintain currency of threat condition and determine which security issues may have an impact on the organization
- Enter event/incident reports received from the constituency into the incident management knowledge base
- Provide proper training and awareness for constituents to identify anomalies and report them (for investigation and resolution)
- Collect incident data and intrusion artifacts (e.g., malware, logs) (to enable mitigation of incidents)
- Perform initial, forensically sound collection of images (for forensic analysis, investigation)
- Maintain a chain of custody of collected evidence following best practices
- Identify missing data or additional sources of information and artifacts

Triage and Analysis (28%)

- Determine whether or not an event is actually an incident
- Categorize events (using the organization's standard category definitions)

- Perform correlation analysis on event reports (to determine if there is affinity between two or more events)
- Perform event correlation using information gathered from a variety of sources within the network environment or enclave to gain situational awareness and determine the effectiveness of an observed attack
- Prioritize events (includes determining scope, urgency, and potential impact)
- Assign events for further analysis, response, or disposition/closure
- Enter information gathered in the preliminary analysis, triage process, and event disposition into the incident knowledge base
- Determine cause and symptoms of the incident
- Document incident analysis in a report or in the incident knowledge base
- Analyze intrusion artifacts and malware (e.g., malware, source code, Trojan horse programs, etc.) (to understand their purpose and/or to identify the specific vulnerability)
- Use malware analysis findings to enable mitigation or prevention of potential incidents
- Perform forensics analysis on constituent systems and networks
- Report digital evidence analysis findings and results to appropriate resources (e.g., stakeholders)
- Coordinate, interface, and work under the direction of appropriate entities (e.g., legal, investigations) regarding investigations or other legal requirements, including investigations that involve external governmental entities (e.g., international, national, state, local)
- Advise on the suitability of Standard Operating Environment's (SOE) baseline standard for forensic analysis
- Perform vulnerability analysis
- Determine the risk, threat level, or business impact of a confirmed incident
- Perform fusion analysis (analyze data from disparate sources to identify concerted attacks and shared vulnerabilities)
- Conduct retrospective analysis

Response (40%)

- Develop an incident response strategy and plan (to limit incident effect and to repair incident damage)
- Perform real-time incident response tasks (e.g., direct system remediation) (to support deployable incident response teams)
- Maintain a deployable incident handling toolkit (e.g., specialized software / hardware) (to support incident response team missions)
- Back up the system
- Determine the risk of continuing operations
- Improve defenses
- Monitor the systems
- Identify relevant stakeholders that need to be contacted or that may have a vested interest or vital role in communications about an organizational incident
- Identify the appropriate communications protocols and channels (media and message) for each type of stakeholder

- Report incidents to appropriate organization management in accordance with organizational guidelines
- Coordinate, integrate, and lead team responses with other internal groups (e.g., IT, management, compliance, legal, human resources, etc.), according to applicable policies and procedures
- Report incidents to law enforcement as required
- Serve as technical experts and liaisons to law enforcement personnel (e.g., to explain incident details, provide testimony, etc.)
- Report and coordinate incidents with the intelligence community as appropriate (to correlate threat assessment data)
- Track and document incidents from initial detection through final resolution
- Provide constituents with security education, training, and awareness

Sustainability (8%)

- Maintain trusted relationships with other internal organizational experts who can give technical and non technical advice and information
- Develop trusted relationships with external experts (incident response teams, vendors, other entities, etc.)
- Monitor and review various forms of media (to ensure that incident management personnel stay abreast of emerging technologies)
- Monitor incident management systems and networks
- Perform risk assessments on incident management systems and networks
- Run vulnerability scanning tools on incident management systems and networks
- Maintain incident monitoring tools, such as intrusion detection systems, intrusion prevention systems, network mapping software, and monitoring / logging systems
- Quantify and monitor the types, volumes, and costs of incidents
- Perform quality assurance (to ensure quality of work and delivery for provided products and services)
- Collect, analyze, and report incident management measures / metrics (to assess the efficiency and effectiveness of incident management activities)
- Examine the effectiveness of penetration testing and incident response tests, training, and exercises
- Assess the effectiveness of communications between the incident response team and related internal and external organizations, and implement changes where appropriate
- Identify incident management improvement actions / recommendations based on assessments of the effectiveness of incident management procedures

Taking the Certification Exam

The allotted examination period for completion of the CSIH exam is three (3) hours.

Test Center Rules

To ensure a fair and consistent testing experience for all candidates, the following rules are enforced at all test centers.

- Candidates should arrive at the test center at least fifteen (15) minutes before the scheduled start time for the examination.
- Candidates must present two (2) forms of identification in order to be admitted into the examination facility. The primary form of identification must be an unexpired government-issued identification with the bearer's picture and signature (e.g., a driver's license or passport). Candidates who do not have the proper identification will not be allowed to take the examination. Social Security cards are not considered to be valid forms of identification.
- Admission to the test center is by appointment only. Candidates must be present at the correct time and location of their appointments to be admitted.
- Candidates must present the proctor with a printed copy of the email message with the Candidate Authorization Code. The proctor will not be able to launch the exam without this code.
- No test materials, documents, or memoranda of any kind may be taken into or out of the test room.
- Candidates may not take food, drinks, tobacco products, chewing gum, purses, briefcases, notebooks, calculators, pagers, cellular telephones, recording devices, photography equipment, or any device with memory capabilities into the testing room. Personal possessions such as cellular phones, briefcases, or backpacks may be collected by the proctor, stored in a secured area, and returned after the test session.
- There are no breaks scheduled during the exam. Candidates who need to leave the testing room to take a break will not be given extra time to finish the exam, and must present ID to sign out of and re-enter the test room.
- It is expressly forbidden to disclose, publish, reproduce, or transmit any part of the exam in any form or by any means, verbal or written, for any purpose, without the express written permission of the certifying organization. Violation may result in civil or criminal prosecution.

After the Certification Exam

The Exam Score

The exam consists of 65 multiple-choice questions. The subject matter distribution for the questions is shown on page 16 of this guidebook.

How the Passing Score was Set

The passing score for the multiple-choice portion of the exam was determined by means of a passing point study using the modified Angoff method carried out by the SEI Certification Program. This technique, which was introduced in 1971 by William Angoff, a measurement research statistician, is one of the most commonly used criterion-based methods for determining the passing score of licensure and certification examinations.

The content for the examination was determined using a panel of content experts, consisting of randomly-selected CSIH professionals with expertise and experience, who meet to discuss the eligibility requirements for the certification, review the job-related tasks in the functional areas of the job-task analysis, and develop a composite profile of a typical minimally-qualified candidate. From these profiles, a list of job-related behaviors is developed to distinguish a candidate who is minimally qualified from one who is below the certification standard.

The list of job-related behaviors is used to develop a test specification that delineates the number of questions from each of the functional areas to be included on the exam. Qualified subject matter experts were trained in techniques for developing clear, non-trivial questions to test the knowledge and skills required for minimum performance as a Computer Security Incident Handler. Upon completion of the question writing process, other subject matter experts were asked to review the questions for clarity, correctness, and appropriateness. Questions were extensively critiqued, rewritten if necessary, and, where appropriate, rejected from inclusion in the question bank. All of the questions in the question bank underwent the same rigorous review process by multiple reviewers.

The cut score study was then conducted by the panel of subject matter experts, who first discussed how to rate each exam question, then individually rated the exam question in terms of how many of the minimally-qualified candidates would answer each question correctly. These ratings were then used to determine the passing scores by averaging the panel's ratings for each item and summing the averages across panel members.

Notification of Results

Official test results will be sent by email no later than thirty (30) days after the exam date.

Successful candidates will receive a welcome kit that contains the certification certificate and other information pertinent to holders of SEI certifications. The welcome kit will be sent to the primary home or work address submitted on the candidate's application.

Certificates

All candidates who successfully complete the qualifications for the CSIH certification will receive an official certificate bearing the date of the final qualifying event. The certificate will also display the certificant's name as entered on the original certification application, unless the certificant subsequently submitted a request for name change. The certificate will bear a unique registration number and the expiration date of certification, which shall be three years from the last day of the month in which certification was granted.

Retaking the Exam

Candidates who do not pass the certification examination on the first attempt may retake the examination up to two (2) additional times within twelve (12) months of the initial attempt. All retakes have the same exam fee (\$499 USD) as the initial attempt.

Candidates who do not pass the examination after three (3) attempts must wait for two (2) years and show evidence of further incident handling and/or security experience and knowledge before reapplying for certification.

Recertification

Recertification is a mechanism for ensuring that certified professionals have maintained or increased their knowledge and skills during the certification period and that they are up-to-date on current industry standards. The CERT-Certified CSIH credential is valid for a period of three (3) years from the award date; at the end of that time, certification holders must apply for recertification.

Recertification Requirements

Certified individuals are required to renew their certification according to the following renewal requirements.

- Submit the renewal application packet with supporting documentation to the SEI; all renewal criteria must be completed and submitted to SEI at least thirty (30) days prior to the last day of the month in which the certification will expire
- Remit the renewal fee of \$150.00 (USD)
- Demonstrate evidence of ongoing active engagement in the practice of computer security incident handling, in professional growth activities, and in expansion of skills through completion of at least sixty (60) Professional Development Units (PDUs), as described below

Professional Development Units (PDUs)

A Professional Development Unit (PDU) is a measuring unit used to quantify learning and development activities. One (1) PDU is earned for every one (1) hour spent in a planned structured experience or activity within the limits set by the SEI for each category of professional activity (see below). To maintain a balance, some activities have a maximum number of credits that can be allotted towards the renewal criteria.

The SEI requires certified professionals to obtain PDUs in the interval between certification award and recertification to ensure that certificants maintain their technical skills and abilities and are aware of emerging technologies and processes associated with incident handling activities. CSIH professionals are encouraged to select PDU activities that will expand or complement their knowledge and skills. The SEI Certification Program Manager does not pre-approve PDUs. CSIH professionals are responsible for ensuring that professional activities meet the renewal criteria.

Activities that qualify for PDU credit are divided into four categories, as described on the following page.

1. Professional activities (maximum of 40 PDUs per renewal cycle)

One (1) hour of professional activity in the field of computer security incident handling earns one (1) hour of PDU credit as approved by the SEI. Professional activities include the following.

- Participation in a CSIRT or performance of incident management tasks for at least 25% of full-time work activities
- Completion of in-house seminars, training, or educational classes
- Attendance at approved association or society meetings

2. Continuing education (maximum of 23 PDUs per renewal cycle)

PDUs are awarded for formal academic or professional education where computer security is the primary topic of instruction, according to the following scheme.

- Completion of one (1) semester hour (2.5 hours per week in a 15-week course) earns 15 PDUs
- Completion of one (1) academic quarter hour (2.5 hours per week in a 10-week course) earns 10 PDUs
- Completion of one (1) CEU earns 10 PDUs
- Completion of a course or seminar offered by SEI, an SEI Transition Partner, or training provider as approved by the SEI earns one (1) PDU for each one (1) contact hour

3. Teaching, presentations, and development (maximum of 20 PDUs per renewal cycle)

- One (1) hour of teaching courseware that is directly related to computer security incident handling earns one (1) PDU; teaching credit is awarded for courses taught the first time during the renewal cycle
- One (1) hour of participation in the development of course curricula earns one (1) PDU for each activity
- One (1) hour of speaking or presenting at a conference, seminar, or society meeting earns one (1) PDU per activity
- One (1) hour of participation in the development of presentations for conferences, seminars, or society meetings earns one (1) PDU per activity

4. Authoring activities (maximum of 30 PDUs per renewal cycle)

- Authoring or co-authoring an article related to computer security incident handling that is published in an SEI-approved journal or magazine earns 10 PDUs per activity
- Authoring or co-authoring a book or textbook that pertains to computer security that is published within the renewal cycle earns 20 PDUs per activity
- Authoring, co-authoring, or acting as contributing editor to an online newsletter that pertains to computer security earns 10 PDUs per activity

NOTE: CSIH professionals who author or co-author publications should forward a copy to the SEI Certification Program Manager or provide information on how to obtain a copy of the work.

be contacted to discuss any discrepancies or adjustments in the number of earned PDUs and/or will be asked to delete any entries that do not meet the renewal criteria. If a Renewal Activity Log is rejected, the CSIH professional will be notified and will have sixty (60) days to provide additional supporting documentation, to obtain additional PDUs, or to correct any discrepancies in the Renewal Activity Log.

SEI Audit of the CSIH Certification Renewal Program

The SEI Certification Program Manager will audit a random number of submitted logs each year. This helps to ensure that the quality of activities submitted continue to meet certification program requirements. CSIH professionals who are selected for an audit will be notified by letter and may be asked to supply additional information or supporting documentation as it relates to their individual Renewal Activity Log. The goal is to audit 2% to 3% of the total number of certificants in a fiscal year.

SEI Certification Program Policies

Policy on the Code of Professional Conduct

All professionals who are certified by the SEI recognize that such certification is a privilege that must be both earned and maintained. In support of this principle, all SEI-Authorized and -Certified professionals are required to commit to fully support the Code of Professional Conduct (COPC). Certified or registered professionals who intentionally or knowingly violate any provision of the COPC will be subject to action by a peer review panel, which may result in the revocation of certification. The SEI Code of Professional Conduct is available online at the following site:

<http://www.sei.cmu.edu/pub/documents/04.reports/pdf/04sr009.pdf>.

Policy on Ethics

In order to maintain their certification, all certified and registered professionals will be required to successfully comply with all rules and requirements for conduct in an ethical manner, as outlined in the Code of Professional Conduct.

Policy on Governance

Before the SEI can grant certification under any of its certification programs, candidates must agree and communicate in writing that they agree to the terms and conditions of the Certification Agreement. This document is part of the application package.

Policy on Conflict of Interest

A conflict of interest is defined in the Code of Professional Conduct for SEI Services as two or more competing priorities that may compromise the objectivity of an authorized or certified professional, candidate, or SEI Partner. If a situation involving a conflict of interest is inherent or cannot be avoided, the individual should disclose the conflict to the SEI by using the Conflict of Interest Disclosure Form at

<http://www.sei.cmu.edu/partners/conflict-form.html>.

Policy on Confidentiality, and Privacy Statement for Data Collected

The SEI collects some data online via the SEI website. Because the SEI website was created in the United States and does not necessarily comply with laws of any other

country, certificants must review these statements before submitting any data through this site. This privacy statement is incorporated into and subject to the Terms of Use found at <http://www.sei.cmu.edu/about/disclaimer.html>. Reference information can be found at <http://www.sei.cmu.edu/about/privacy.html>

Policy on Certification Documentation and Materials

All qualification event applications, status, and results will be kept confidential by the SEI at all times. Application materials and examination results will be kept in a secure manner at the SEI offices in Pittsburgh, PA. Individuals who have access to secured materials must be employees of the SEI. All employees, volunteers, and exam consultants must read and sign the SEI COPC statement and a non-disclosure agreement (if deemed necessary).

A directory of certified individuals will be published on the SEI website. Certified individuals who do not want to have their names and certification status published must communicate this request in writing to the SEI Certification Program.

Policy on the Family Educational Rights and Privacy Act (FERPA)

Certification records created at Carnegie Mellon University are strictly confidential and their protection is mandated under federal legislation known as the Family Educational Rights and Privacy Act of 1974 (FERPA). More information about the SEI and FERPA is available at <http://www.sei.cmu.edu/partners/ferpa/index.html>.

Policy on Logos, Service Marks, and Trademarks

Certified professionals may use the CERT-Certified Computer Security Incident Handler title and logo on business cards and documents (such as slide sets, web pages, or Usenet posts) within the parameters of the SEI guidelines. These guidelines for proper reference to and use of SEI and CMU logos, service marks, and trademarks, and instructions on use of superscripted service mark and trademark symbols (or substitute service mark and trademark designators) can be found at <http://www.sei.cmu.edu/about/legal-trademarks.html>. Any complaints or reports of misuse should be reported to SEI-Certification via certification-info@sei.cmu.edu.

Policy on Examination Irregularities

It is the policy of the SEI Certification Program that any receipt, possession, or transmission of examination materials (including examination questions and cases in

any form), either before the examination, or on-site during the exam, or in the future, is a breach of SEI Certification policy and is strictly forbidden. The SEI reserves the right to take whatever measures are necessary to protect the integrity of its examinations. This includes, but is not necessarily limited to, exclusion from a current examination, revocation of certification, and/or suit for recovery of damages.

Policy on Examination Score Validity

The validity of scores awarded to candidates for their performance on a certification examination is protected by every means available. Any SEI staff or designee who observes or discovers candidates engaging in irregular activity is obligated to report the individual(s) and the observed behavior to the SEI Certification Program office. The performance of all candidates is monitored and may be analyzed statistically for the purpose of detecting invalid scores. Any evidence by observation, discovery, or statistical analysis that suggests one or more candidate scores may be invalid because of irregular behavior will result in the SEI Certification Program office withholding the scores pending further investigation, and affected candidates will be so notified.

Examples of irregular behavior that might affect the validity of scores and might necessitate the withholding of scores pending further investigation include, but are not limited to the following.

- Copying answers from another candidate
- Permitting one's answers to be copied
- Discussing the specific content of an examination with one or more fellow candidates at any time before, during, or after the administration of an examination
- Unauthorized possession, reproduction, recording, transmission, or disclosure of materials or other information regarding the content of an examination at any time before, during, or after the administration of an examination
- Other evidence indicating that the security of an examination has been compromised

Upon analysis of all available information in such circumstances, the SEI Certification Program office will determine the validity of the examination scores in question and will notify affected candidates. If it is determined that the scores in question are invalid, the scores will not be released and the candidates will be so notified.

Candidates or other persons who are directly implicated in an irregularity affecting the validity of exam scores will be subject to additional sanctions, including permanently barring the individual(s) from all future examinations, terminating a candidate's participation in an ongoing examination, invalidating the results of the candidate's examination, withholding or revoking a certification, terminating any existing relationship with SEI, and any other action deemed appropriate.

SEI certification candidates and other persons who are deemed subject to additional sanctions will be provided with a written notice of the charges and an opportunity to respond to such charges in accordance with the appeals policy and procedures established by the SEI.

Policy on Requests for Exam Rescoring

Candidates who feel that their examinations may have been incorrectly scored may submit a written request for rescoring within 60 days of receiving their initial test scores. The request must be accompanied by a \$75 rescoring fee and submitted to the CSIH Certification Program Manager, SEI Certification Program, 4500 Fifth Avenue, Pittsburgh PA 15213. The CSIH Certification Program Manager will inform the candidate in writing of the outcome of the rescoring effort. Should a candidate decide to appeal the examination score, it will be reviewed by the CSIH Advisory Board in accordance with the Policy on Appeals of Adverse Decisions, and all board decisions will be final.

Policy on Appeals of Adverse Decisions

Individuals who disagree with an adverse decision of the SEI Certification Program have the right to appeal. Such adverse decisions may include

- rejection of application
- determination of ineligibility for certification
- denial of requests for special exam accommodations
- denial of certification or recertification
- revocation or suspension of certification

Individuals may appeal an adverse decision to the Certification Program by using the appeals procedure delineated below.

1. All appeals must be presented in writing to the CSIH Certification Program Manager, SEI Certification Program, 4500 Fifth Avenue, Pittsburgh PA 15213.
2. The appeal must contain all information and documentation in support of the claim that the CSIH Certification Program made an erroneous decision to reject the application.
3. The written request for appeal must be postmarked within thirty (30) calendar days from the date on the written notification from the CSIH Certification Program containing the adverse decision.
4. The appeal and supporting documentation must be sent to the CSIH Certification by certified mail.

Upon receipt of the appeal and supporting documentation, the CSIH Certification Program Manager shall promptly notify the CSIH Advisory Board of the appeal. The Certification Program Manager will investigate the basis and background for the

appeal, and will meet with the CSIH Advisory Board to discuss and rule on the appeal. The Certification Program Manager will inform the appellant in writing of the outcome of the appeal. If the appeal is found to be without merit, the decision of the CSIH Advisory Board will be final and may not be appealed further.

Revocation, Suspension, Expiration, or Surrender of Certification

Revocation of Certification

The SEI Certification Program may revoke an individual's certification under one or more of the following circumstances.

- The certification was granted contrary to the rules and regulations of the SEI
- The certification was granted to a person who was not eligible to apply for certification
- The certificant has failed to abide by all rules, regulations, and standards covering the certification programs promulgated by the SEI
- The certificant no longer meets the qualifications established by the SEI
- The certificant has been disciplined, reprimanded, or suspended

Prior to the revocation of a certification, the SEI Certification Program Manager shall advise the certificant of the proposed action, the reasons therefore, and the certificant's right to file a written response. Such notice will be provided in writing by certified mail (with return receipt requested) to the certificant's last known address on file with the SEI. The certificant's written response must be received by the SEI within thirty (30) days after the date of the notice.

Once a written response is received, the SEI Certification Program Manager will request an interview with the certificant in order to review his/her petition. At the end of the thirty (30) day response period, the SEI Certification Program Manager will present the petition and findings to the CSIH Certification Advisory Board. The Board shall meet to consider the grounds for revocation, the certificant's response (if any), and any additional information available, and will decide whether or not to revoke the certification. The petitioner may attend the revocation hearing to present his/her petition. The certificant will be advised in writing of the decision.

If the Certification Program revokes a certificant's certification, the individual must immediately surrender to the Certification Program Manager the original copy of the official certification certificate and all copies thereof. Furthermore, the individual must immediately cease to use any logos or marks as detailed in the Certification agreement.

Suspension of Certification

The certification of any certificant shall be automatically suspended without prior notice if the certificant has

- failed to complete the required renewal activities by the end of the certification validity period

- been suspended pending an investigation of reported violations of the COPC or of any other irregular behavior

The SEI Certification Program Manager shall notify the certification holder in writing of the suspension of certification and of the certification holder's right to petition for reinstatement. However, suspension shall be automatic upon the occurrence of an event within that scope, regardless of whether the notice of suspension has yet been transmitted.

Reinstatement of Certification after Suspension

After a certification has been suspended, the certification holder may petition the SEI Certification Program for reinstatement of the certification. The petition may be informal, but it must be in writing and must adequately identify the following information.

- Reason(s) for the suspension
- Effective date of the suspension
- The reasons for which the certification holder believes that the certification should be reinstated
- The relief or remedy requested

If the suspension decision is upheld, the formerly-certified individual must immediately cease advertisement or representation to the public as being certified by the SEI and also must surrender the certificate of certification to the SEI Certification Program office.

Expiration of Certification

Failure of a certification holder to file a properly completed Renewal Log in a timely manner at the end of the certification period will result in the expiration of the certification. The SEI Certification Program will provide the certification holder with written notice by email of the certification expiration and shall advise the certification holder of the right to file a written response.

The certification holder may provide written documentation to overcome or cure the pending expiration, provided that the documentation is received at the SEI Certification Program office within thirty (30) days after the date of the expiration notice. If timely response is not provided to the SEI Certification Program, the certification shall be deemed to have expired, and no further notice need be given to the formerly-certified individual.

Resignation and Voluntary Surrender of Certification

A certification holder may resign as a certified Computer Security Incident Handler and voluntarily surrender certification by notifying the SEI Certification Program in writing. Unless otherwise directed by the certification holder, so long as the certification holder remains eligible for certification, such resignation shall be immediately effective. The former certification holder must immediately cease advertisement or representation to the public of being certified by the SEI and must surrender the certificate of certification to the SEI Certification Program office.

Appeals of Decisions to Revoke or Suspend Certification

Individuals may appeal the decision of the SEI Certification Program to deny, revoke, or suspend certification. The complete appeals policy and procedure can be found on page 30 of this guidebook.

Appendix A:

Completion Guidelines for the CSIH Application Form

Name

For security purposes, two forms of identification are required for entrance to the certification exam. Candidates must have an unexpired government-issued ID that matches the name on the application. Candidates whose government-issued ID does not match the name on the application will not be allowed to sit for the examination and will forfeit the test fee. Therefore, applicants should ensure that the name entered on the application form exactly matches the name on the government-issued ID that will be used at the test center as proof of identity.

Date of Birth

For security purposes, candidates must have an unexpired government-issued ID containing the individual's date of birth; the dates on the application and on the identification used for examination entrance must match exactly.

Job/Position

Applicants should use their current job title or position description title for this item on the application form.

Employer

Applicants should provide the name of the company or organization with whom they are currently employed for this item on the application form.

Employer Address/Employer Phone/Contact Information Street Address and Mailing Address

Official communications and certification certificates are mailed to a candidate's primary address. Therefore, applicants should list the primary address (work or home) to which they would like certificates and other certification materials to be sent. Applicants who would prefer to have certificates and other information sent to their home should provide a current street address (for both postal and private courier service deliveries) and current mailing address (if different from the home address).

Daytime and Evening Telephone Numbers

Applicants should provide relevant telephone numbers (in case these are needed for private courier delivery service) for this item on the application form.

Recommendation Letter

Applicants must provide a letter of recommendation from their current manager. The letter must be accompanied by a recommendation form (see Appendix C), and both should be sent directly to the SEI in accordance with the submission instructions on the recommendation form.

Required Application Attachments for Submission

Applicants also must include the following documents with the completed application.

- A current resume that includes appropriate professional experience (see the following section of these instructions for examples of experience that meets the application criteria)
- A signed copy of the SEI Code of Professional Conduct (see Appendix D, or download from http://www.sei.cmu.edu/partners/files/copc_form_indiv.pdf)

Professional Experience that Meets the Criteria for Application

Experience in incident management can cover a wide spectrum of tasks, including initial detection or reporting of a security event or incident, categorization or prioritization of reports, analysis of incidents and events, determination of appropriate response strategies, performing the actual response, resolution of the incident, communicating with appropriate individuals throughout the process, and documenting or recording actions taken.

Specific professional experience that satisfies the CSIH application criteria includes the following.

- Activities involved in operating and/or managing a CSIRT, or working in a security operations center or network operations center
- Teaching courses in incident, vulnerability, or artifact handling
- Taking action to protect systems and networks affected or threatened by intruder activity (such as filtering network traffic, patching or repairing systems, and rebuilding systems)
- Collecting evidence (following established rules of evidence)
- Performing computer forensic analysis on compromised systems (following established rules of evidence)
- Performing artifact analysis or malicious code analysis
- Analyzing networks and systems to look for security weaknesses, anomalous activity, or intruder activity
- Providing solutions, mitigation strategies, or work-arounds through hands-on assistance or via alerts, bulletins, advisories, technical documentation, web sites, phone calls, emails, or other dissemination mechanisms
- Coordinating response efforts and incident data exchanges
- Coordinating and collaborating with management, legal, law enforcement, and other internal or external organizations

- Coordinating communications with stakeholders involved in computer security events and incidents such as affected individuals, management, and other internal or external organizations

SEI Certification Agreement

Applicants must agree to abide by the terms of the SEI Certification Agreement, as included on the CSIH Application Form. After reading the form, the applicant should affix his or her signature, address, and the date in the spaces indicated on the application form.

Incomplete Applications

Incomplete applications will be returned to the applicant. Applicants who submit an incomplete application will receive an email from the CSIH Certification Program Manager indicating the materials or information needed to make the application complete. If the recommendation form does not meet the required standard, the Certification Program Manager will inform the candidate that another recommendation form is necessary in order for the application to proceed in the review process.

*Required information

Required Application Attachments for Submission

- Copy of a current resume. List your relevant work experiences chronologically, starting with the most recent.

- Completed Code of Professional Conduct (COPC) form that can be downloaded from http://www.sei.cmu.edu/partners/files/copc_form_indiv.pdf.

SOFTWARE ENGINEERING INSTITUTE CERTIFICATION AGREEMENT

1 PURPOSE

The Software Engineering Institute (“SEI”) is a Federally Funded Research and Development Center operated by Carnegie Mellon University that performs work under a contract sponsored by the United States Department of Defense. As part of its work, the SEI identifies, develops and advocates practices for developing, acquiring, and delivering high quality software products and services and protecting networked systems. In furtherance of its mission to transition technology, the SEI grants certifications to individuals who demonstrate proficiency in a specific set of skills, abilities and knowledge relative to a particular technology area.

You desire to become SEI-Certified with respect to one or more Programs (as defined herein) and agree to be legally bound by the terms and conditions contained in this Certification Agreement (this “Agreement”).

2 DEFINITIONS

- (a) “Certification(s)” means the status achieved with respect to one or more of the Programs offered by the SEI.
- (b) “Marks” means the marks reflected on the SEI website at <http://www.sei.cmu.edu/about/legal-trademarks.html> that are associated with the Program for which Certification is obtained.
- (c) “SEI-Certified” means an individual who has successfully met the requirements for obtaining and maintaining Certification as set forth in Section 3.
- (d) “SEI Partner” means an organization that is selected by the SEI, licensed by the SEI under a written agreement between the SEI and such organization to deliver certain SEI courses and/or services, and monitored by the SEI.
- (e) “Program(s)” means one or more of the certification programs offered by the SEI under this Agreement as reflected on the SEI website at <http://www.sei.cmu.edu/certification/>. Each program includes a formally documented process whereby individuals may become SEI Certified.

3 CERTIFICATION

- (a) Certification Requirements. In order to obtain and maintain Certification, you must:

- (i) Follow the application process and pay the requisite fee for the relevant Program as described on the SEI website at <http://www.sei.cmu.edu/certification/> and
- (ii) Meet all requirements of the relevant Program including, but not limited to, pre-requisites, training requirements, testing, continuing education, professional conduct policies, and recertification requirements, all of which are set forth on the SEI website at <http://www.sei.cmu.edu/certification/>. SEI reserves the right to change the Program and/or the Program's requirements at any time without cause and without notice. SEI also reserves the right to discontinue any Program for any reason at any time; and
- (iii) Agree in writing to abide by the SEI's Code of Professional Conduct ("COPC"), a copy of which has been provided to you and is set forth on the SEI website at <http://www.sei.cmu.edu/partners/copc.html>; and
- (iv) Remain sponsored by an SEI Partner (if applicable); and
- (v) Abide by the quality guidelines for the relevant Program as set forth on the SEI website at <http://www.sei.cmu.edu/certification/governance.html>; and
- (vi) Execute or electronically accept the terms of this Certification Agreement and any new versions or updates to such Certification Agreement at such times as the SEI may request.

(b) Issuance of Certificate. Once you have met all of the criteria for the relevant Program or Programs, including the acceptance of this Agreement, the SEI will issue a Certificate or Certificates to you evidencing that you are SEI-Certified for the particular Program or Programs.

(c) Expiration of Certification/Renewal Requirements. Certifications for most Programs expire three (3) years after issuance and must be renewed in accordance with the renewal criteria for the relevant Program as set forth on the SEI website at <http://www.sei.cmu.edu/certification/>. Notwithstanding anything in this Agreement to the contrary, the SEI has the right to refrain from granting or renewing your Certification if the SEI believes that your Certification or use of the Marks will adversely affect the SEI.

4 TERM AND TERMINATION

Term. This Agreement becomes effective when you submit a signed form or click the "I agree" button. Your certifications shall become effective on the date on which you receive notice from the SEI that you have met all the requirements necessary to receive Certification in a particular Program and shall continue in effect until all of your SEI Certifications have expired or have been revoked, subject to suspension as provided below.

5 SUSPENSION OF CERTIFICATION

- (a) Causes for Suspension. The SEI may suspend one or more of your Certifications, upon written notice to you, effective as of the date specified in such notice, if:
 - (i) The SEI determines, in its sole discretion, that the quality of your delivery of SEI services does not meet the quality guidelines for the relevant Program as set forth on the SEI website at <http://www.sei.cmu.edu/certification/governance.html> or
 - (ii) You have failed to follow the policies, procedures, and methods as specified by the Program; or

- (iii) You are delinquent in the payment of any fees due to the SEI; or
- (iv) You are no longer sponsored by an SEI Partner (if applicable); or
- (v) You are in breach of any of the terms of this Agreement and you fail to cure such breach within fifteen (15) days after written notice from the SEI.

(b) **Effect of Suspension.** Upon the effective date of your suspension, all of your rights to deliver SEI services under the relevant Program shall be suspended and you shall be prohibited from delivering those services unless and until your suspension is lifted by the SEI. In addition, the SEI shall notify your sponsoring SEI Partner of your suspension.

(c) **Remediation.** If one or more of your Certifications is suspended:

- (i) Within fifteen (15) days of the SEI's notice of suspension to you, SEI will furnish you with an outline of remedial actions that you must take in order for the SEI to consider lifting your suspension; and
- (ii) Promptly after your receipt of such remedial action outline, you must notify the SEI that you will begin such remedial actions specified and that you will complete such actions within the designated time frame.
- (iii) If the SEI, in its sole discretion, is satisfied with the remedial actions taken by you, the SEI may lift the suspension of your Certification by written notice to you.

6 REVOCATION OF CERTIFICATION

(a) **Causes for Revocation.** The SEI may revoke one or more of your Certifications, upon written notice to you, effective as of the date specified in such notice, if:

- (i) While under suspension, you fail to complete the recommended remedial actions to the satisfaction of the SEI; or
- (ii) You have failed to follow the policies, procedures, and methods as specified by the Program; or
- (iii) You have had one or more Certifications (whether for the same or different Programs) suspended two (2) times prior to the recent event requiring suspension; or
- (iv) You have participated in any action that compromises the integrity and confidentiality of any examination or the relevant Program quality component, including but not limited to a breach of the COPC. In the event that revocation is due to a violation of the COPC, your Certifications in all SEI Programs shall be revoked.

(b) **Effect of Revocation.** Upon the effective date of your revocation:

- (i) Your right to deliver SEI services under the relevant Program is terminated; and
- (ii) Your right to use the Marks relating to the relevant Program is terminated; and
- (iii) Your right to use the credential "SEI-Certified" (relating to the relevant Program) is terminated; and
- (iv) Your name will be removed from the SEI Partner Directory as an SEI-Certified individual of the relevant Program; and

- (v) In the event revocation is due to a violation of the COPC, your Certifications in all Programs shall be revoked and you shall be barred from applying for SEI Certification for any Program in the future.

7 REVIEW AND APPEALS PROCESS

In the event that your Certification is suspended or revoked, you may be permitted to appeal such suspension or revocation. In such event, you must follow the review and appeal procedures applicable to the relevant Program as set forth on <http://www.sei.cmu.edu/certification/governance>.

8 CONFIDENTIALITY AND INTELLECTUAL PROPERTY OWNERSHIP

(a) Confidentiality. You agree to retain in confidence all information and know-how obtained from the SEI during the Certification process and during your tenure as an SEI-Certified individual. This information includes, but is not limited to, certification materials and exam questions. You agree that the contents of all Certification exams are confidential and that the disclosure of any such information would compromise the integrity of the Program and of Certifications and, therefore, any such disclosure may result in the revocation of your Certification or Certifications, in addition to all other legal and equitable actions available to the SEI. Your obligations of confidentiality hereunder shall survive the expiration or termination of this Agreement.

(b) Intellectual Property Ownership. SEI retains all rights, title and interest in and to all Programs and related information, content, data, exams, materials, and all copyrights, patent rights, trademark rights and other proprietary rights therein.

(c) Use of Marks. Subject to the terms and conditions of this Agreement, the SEI grants to you a non-exclusive and non-transferable license to use the Marks relating to the Program Certification(s) that you have earned in accordance with the guidelines set forth on <http://www.sei.cmu.edu/about/legal-trademarks.html>. You may not use any such Marks until the SEI has notified you in writing that you have achieved Certification status for the particular Program or Programs.

9 LIMITATION OF LIABILITY/INDEMNIFICATION

(a) ANY AND ALL INFORMATION, MATERIALS, SERVICES, INTELLECTUAL PROPERTY AND OTHER PROPERTY AND RIGHTS GRANTED AND/OR PROVIDED BY SEI TO YOU ARE GRANTED AND/OR PROVIDED ON AN "AS IS" BASIS. SEI MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, AS TO ANY MATTER, AND ALL SUCH WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE EXPRESSLY DISCLAIMED. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, SEI DOES NOT MAKE ANY WARRANTY OF ANY KIND RELATING TO EXCLUSIVITY, INFORMATIONAL CONTENT, ERROR-FREE OPERATION, RESULTS TO BE OBTAINED FROM USE, FREEDOM FROM PATENT, TRADEMARK AND COPYRIGHT INFRINGEMENT AND/OR FREEDOM FROM THEFT OF TRADE SECRETS. YOU ARE PROHIBITED FROM MAKING ANY EXPRESS OR IMPLIED WARRANTY TO ANY THIRD PARTY ON BEHALF OF SEI RELATING TO ANY SEI PROGRAMS, MATERIALS OR PRODUCTS.

SEI SHALL NOT BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY REASON WHATSOEVER ARISING OUT OF OR RELATING TO THIS AGREEMENT (INCLUDING ANY BREACH OF THIS AGREEMENT) FOR ANY DAMAGES WHATSOEVER, INCLUDING BUT NOT LIMITED TO LOSS OF PROFITS OR FOR INCIDENTAL, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES, EVEN IF SEI HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR HAS OR GAINS KNOWLEDGE OF THE EXISTENCE OF SUCH DAMAGES.

(b) Indemnification. You agree to defend, indemnify and hold harmless SEI and its trustees, officers, employees, attorneys and agents from and against any and all liability, damage, loss or expense (including reasonable attorneys fees and expenses) incurred by or imposed upon any of SEI and/or its trustees, officers, employees, attorneys and agents in connection with any claim, suit, action or demand arising out of or relating to any exercise of any right or license granted or provided to you under this Agreement or and Certification Program under any theory of liability (including without limitation, actions in the form of tort, warranty, or strict liability, or violation of any law, and regardless of whether such action has any factual basis).

10 ASSIGNMENTS

You may not assign any rights, licenses or obligations received under this Agreement. Any attempted assignment in violation of this Agreement shall be null and void and without effect.

11 MISCELLANEOUS

(a) Waiver and Modification. You waive any right to challenge the validity and enforceability of this Agreement on the grounds that it was transmitted and entered into electronically. You agree that entering into the Agreement electronically is equivalent to signing the Agreement. Failure by either of us to enforce any provision of this Agreement will not be deemed a waiver of future enforcement of that or any other provision. Any waiver, amendment or other modification of any provision of this Agreement will be effective only if in writing and signed by both you and the SEI.

(b) Severability. If a court of competent jurisdiction finds any provision of this Agreement to be unenforceable, that provision of the Agreement will be enforced to the maximum extent permissible so as to affect the intent of the provision, and the remainder of this Agreement will continue in full force and effect.

(c) Governing Law. This Agreement shall be governed by the laws of the Commonwealth of Pennsylvania without regard to its conflicts of laws provisions.

(d) Disputes. To dispute any decision of the SEI regarding revocation or suspension of Certification, you must exhaust the review and appeals procedures for the relevant Program. Thereafter, all claims and/or controversies of every kind and nature arising out of or relating to this Agreement shall be settled (1) at SEI's election, by binding arbitration administered by the American Arbitration Association ("AAA") in accordance with its Commercial Arbitration Rules and, in such case (a) the arbitration proceedings shall be conducted before a panel of three arbitrators, with each party selecting one disinterested arbitrator from a list submitted by the AAA and the two disinterested arbitrators selecting a third arbitrator from the list, (b) each party shall bear its own costs of arbitration, (c) all arbitration hearings shall be conducted in Allegheny County, Pennsylvania, and (d) the provisions hereof shall be a complete defense to any suit, action or proceeding instituted in any Federal, state or local court or before any administrative tribunal with respect to any claim or controversy arising out of or relating to this Agreement and which is arbitrable as provided in this Agreement, provided that either party may seek injunctive relief in a court of law or equity to assert, protect or enforce its rights in any intellectual property and/or proprietary or confidential information as described in this Agreement, or (2) in the event that SEI does not elect binding arbitration as permitted in point (1) above, exclusively in the United States District Court for the Western District of Pennsylvania or, if such Court does not have jurisdiction, in any court of general jurisdiction in Allegheny County, Pennsylvania and each party consents to the exclusive jurisdiction of any such courts and waives any objection which such party may have to the laying of venue in any such courts.

(e) Notices. It is your responsibility to maintain a current address with the SEI. All notices required to be given to you under this Agreement will be delivered to the last address that you provide to the SEI.

(f) Entire Agreement. This Agreement is the complete agreement regarding the Certification(s) obtained by you and replaces any prior oral or written communications between the SEI and you.

YOU HEREBY REPRESENT TO THE SEI THAT YOU (1) HAVE READ AND UNDERSTAND THE TERMS OF THIS AGREEMENT AND (2) AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THE AGREEMENT; AND (3) ACKNOWLEDGE THAT THE SEI IS RELYING ON SUCH REPRESENTATIONS IN GRANTING CERTIFICATION TO YOU.

Signature and Date

Print Name

Address:

Signatory indicates that the candidate certifies that all of the information included in my application packet is true, complete, and accurate. I understand that all components of my application packet are subject to verification, and I give my permission for any person or entity to provide Carnegie Mellon with information relevant to such verification. I understand that all components of my application packet become the property of the Software Engineering Institute and that they will not be returned to me or duplicated for me. I understand that the application fee is not refundable.

Carnegie Mellon University does not discriminate and Carnegie Mellon University is required not to discriminate in admission, employment, or administration of its programs or activities on the basis of race, color, national origin, sex or handicap in violation of Title VI of the Civil Rights Act of 1964, Title IX of the Educational Amendments of 1972 and Section 504 of the Rehabilitation Act of 1973 or other federal, state, or local laws or executive orders. In addition, Carnegie Mellon University does not discriminate in admission, employment, or administration of its programs on the basis of religion, creed, ancestry, belief, age, veteran status, sexual orientation or gender identity. Carnegie Mellon does not discriminate in violation of federal, state, or local laws or executive orders.

Appendix C:
CSIH Recommendation Letter Submission Form

(This page intentionally left blank.)

| | Top 1% | Top 10% | Top 25% | Top 50% | No Basis for Evaluation |
|------------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| Analysis and problem solving | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Leadership | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Working with others | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Initiative | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Personal integrity | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Please describe the particular strengths and weaknesses of this applicant. _____

Recommendation

Please indicate your opinion about the applicant's admission:

- I enthusiastically recommend this applicant
- I recommend this applicant
- I recommend this applicant with some reservations
- I do not recommend this applicant

Reservations about this applicant: _____

Signature

 Recommender's Signature Date

Submission Instructions

Please place your recommendation form, any supplementary pages, and your business card in a sealed envelope with your signature across the seal. Mail the envelope directly to:

Software Engineering Institute
 Carnegie Mellon University
 Attn: Incident Handler Certification/J. Welch
 4500 Fifth Avenue
 Pittsburgh, PA 15213-3890

Direct any questions to the SEI Certification Program Manager:

Phone: +1 412-268-4024
 Email: certification-info@lists.sei.cmu.edu

Carnegie Mellon University does not discriminate and Carnegie Mellon University is required not to discriminate in admission, employment, or administration of its programs or activities on the basis of race, color, national origin, sex or handicap in violation of Title VI of the Civil Rights Act of 1964, Title IX of the Educational Amendments of 1972 and Section 504 of the Rehabilitation Act of 1973 or other federal, state, or local laws or executive orders. In addition, Carnegie Mellon University does not discriminate in admission, employment, or administration of its programs on the basis of religion, creed, ancestry, belief, age, veteran status, sexual orientation or gender identity. Carnegie Mellon does not discriminate in violation of federal, state, or local laws or executive orders.

Appendix D: SEI Code of Professional Conduct



SEI Code of Professional Conduct Commitment Form for Individuals

All individuals who wish to become authorized or certified must complete this form before being permitted into an advanced training class or before an authorization or certification will be given. If you have any questions, please send email to partner-info@sei.cmu.edu.

Last Name (Family Name) _____
First Name _____ **Middle Name(s)** _____
Phone Number _____ **Email Address** _____

Primary SEI Partner Sponsor Organization (if applicable) _____

SEI Licensed Product Suites (Please check all that apply.)

- CMMI
- Information and Network Security (CERT) (CSIH)
- Software Engineering Measurement and Analysis (IGDM, IPPSS, DPPSS)
- Software Architecture
- TSP

Commitment

- Á I am committed to the Code of Professional Conduct for SEI Services (the Code). I understand that by making this selection, I am agreeing to abide by the Code for all of my current and future SEI authorizations and/or certifications.
- Á I am NOT committed to the Code of Professional Conduct for SEI Services (the Code). I understand that by making this selection, I am not agreeing to abide by the Code. I further understand that my SEI authorizations and/or certifications and/or candidacies will be discontinued with 30 days notice.

Signature _____

Date _____