

SANS

DoD Directive (DoDD) 8570 & GIAC Certification

Date Updated: June 2011



Daryl Gilbertson

National Account Manager
678-714-5712 • DGilbertson@sans.org

Brian Correia

Director
703-968-0103 • BCorreia@sans.org

www.sans.org/8570



What is DoDD 8570?

Department of Defense Directive 8570 provides guidance and procedures for the training, certification, and management of all government employees who conduct Information Assurance functions in assigned duty positions. These individuals are required to carry an approved certification for their particular job classification. GIAC certifications are among those required for Technical, Management, CND, and IASAE classifications.

Who is affected by 8570?

Any full- or part-time military service member, contractor, or local nationals with privileged access to a DoD information system performing information assurance (security) functions – regardless of job or occupational series. The manual, **8570.01M**, specifies that the Department of Defense requires approximately 110,000 identified Information Assurance professionals to be certified within a five year time period. The Defense Information Assurance Program office has divided its Information Assurance workforce into six defined categories (see chart below). The manual also specifies the types of commercial information assurance credentials that qualify for each of the defined categories.

DoD Directive 8570 requires:

- By the end of CY 2010, all personnel performing IAT and IAM functions must be certified.
- By the end of CY 2011 all personnel performing CND-SP and IASAE roles must be certified.
- All IA jobs will be categorized as 'Technical' or 'Management' Level I, II, or III, and to be qualified for those jobs, you must be certified.

Where can I find the 8570 Manual?

- Click on this link: <http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf>
- Contact 8570@sans.org

"As part of the Raytheon IIS Information Security Engineering group, we send nearly all of our new hires through the SANS Security Essentials Bootcamp training classes to ensure they have the fundamental skills necessary to work in our environment. We view GIAC certifications as an essential part of this process. GIAC Certification helps ensure both our management and our customers that our employees understand how to build secure systems."

-MONTY McDUGAL, RAYTHEON



DoD Baseline IA Certifications

TECH II

GSEC†

SEC401: SANS Security Essentials
Bootcamp Style

Security+†

TECH III

GCED†

SEC501: Advanced Security Essentials - Enterprise
Defender

GCIH†

SEC504: Hacker Techniques, Exploits
and Incident Handling

CISSP*†

MGT414: SANS® +S™ Training Program
for the CISSP® Certification Exam

MGT I

GSLC†

MGT512: SANS Security Leadership
Essentials For Managers

GSIF†

SEC301: Intro to Information Security

MGT II

GSLC†

MGT512: SANS Security Leadership
Essentials For Managers

CISSP*†

MGT414: SANS® +S™ Training Program
for the CISSP® Certification Exam

MGT III

GSLC†

MGT512: SANS Security Leadership
Essentials For Managers

CISSP*†

MGT414: SANS® +S™ Training Program
for the CISSP® Certification Exam

Computer Environment (CE) Certifications

GCWN†

SEC505: Securing Windows

GCUX†

SEC506: Securing Linux/Unix

By the end of 2011, all personnel performing CND-SP and IASAE roles must be certified. These courses will prepare you for the required certifications:

Information Assurance System Architecture & Engineering (IASAE) Certifications

CND ANALYST

GCIA†

SEC503: Intrusion Detection In-Depth

CND INCIDENT RESPONDER

GCIH†

SEC504: Hacker Techniques, Exploits, and
Incident Handling

CND AUDITOR

GSNA†

AUD507: Auditing Networks, Perimeters,
and Systems

Computer Network Defense (CND) Certifications

IASAE I

CISSP*†

MGT414: SANS® +S™ Training Program
for the CISSP® Certification Exam

IASAE II

CISSP*†

MGT414: SANS® +S™ Training Program
for the CISSP® Certification Exam

*Or Associate

†SANS training available

Daryl Gilbertson

678-714-5712 (Eastern Time)

DGilbertson@sans.org

DoDD 8570 & GIAC Certification

www.sans.org/8570

Brian Correia

703-968-0103 (Eastern Time)

BCorreia@sans.org

The SANS Promise: You will be able to apply our training the day you get back to the office.



Why is GIAC the best certification for 8570?

The GIAC (Global Information Assurance Certification) Program provides assurance to employers that their employees and contractors can actually do the job they are assigned to do. GIAC goes beyond theory and terminology and tests the pragmatics of Audit, Security, Operations, Management, and Software Security.

The family of GIAC certifications target actual job-based skill sets, rather than taking a one-size-fits-all approach to IT Security. GIAC offers more than 20 specialized information security certifications, many of these certifications are recognized under the DoD 8570 program.

The GIAC certification process validates the specific skills of security professionals and developers with standards that were developed using the highest benchmarks in the industry. There are over 22,000 GIAC certified professionals in the IT Security industry.

Benefits of GIAC Certification for Managers

- Increased confidence that GIAC certified individuals charged with securing your systems, networks, and software applications actually know how to do the job.
- As a proven indicator of job-related knowledge, GIAC certifications help managers ensure they have the right people in the right positions.
- GIAC certification helps to ensure that system and network administrators have the actual technical skills sets needed to meet their security responsibilities.

Benefits of GIAC Certification for Individuals

- GIAC certified professionals possess a job-based skill set that favorably influences job security and advancement.
- GIAC certification identifies those individuals who know the tasks required to protect your systems and networks and who have the skills needed to perform those tasks.
- GIAC ensures that certified professionals can keep their skills and knowledge current through periodic recertification and access to the latest, most up-to-date information.

How GIAC Differs from Other Certifications

- Offers over 20 specialized information security certifications, rather than a one-size fits all approach
- Tests on pragmatics, not theory
- Validates real-world skills
- Ensures knowledge necessary to complete the task at hand

For more information about DoD 8570

- Download a copy of the manual online at www.dtic.mil/whs/directives/corres/pdf/857001m.pdf
- Call the Defense Information Assurance Program (DIAP) Office at **703-604-1480 x112**
- Contact 8570@sans.org



GIAC Exams

GIAC certification exams are administered in an open book and timed format. All GIAC exams are computer based and are required to be taken in a proctored environment. Proctored exam administration is offered through our testing partner, Kryterion, or at your site utilizing education and training officers. For more specific program information, please visit www.giac.org/proctor.

How to Prepare for GIAC Exams

- Reread all the slides and notes sections from your course material two to four times before taking a practice test.
- Create a study index from your course material and your notes. Use index cards and highlighters to help you identify sections with information that is new to you.
- Prepare your open book reference material using tabs and section dividers, so you know where specific content is located
- Listen to the course audio mp3 files.
- Utilize your practice tests. After you study for two to four weeks, take your first practice test and make sure you are on track.

On average, students who pass their GIAC exams put in at least 50 hours of study time, this is study time in addition to classroom training.

Take time to prepare, it will pay off! If you need extra help, consider purchasing a SANS OnDemand package to help you study.

How to Register for GIAC Exams

GIAC exams are not automatically included with SANS training courses. You may add a certification to your training order or you can register for an exam separately.

- To add a certification to your training order, make sure to check the GIAC certification box at the bottom of the registration page.
- If you want to add certification after you have registered, call **301-654-7267**.
- To register for a GIAC certification exam not associated with SANS training, go to www.giac.org/reginfo/challenge.php.

If you have question, e-mail info@giac.org.

"As our C4 systems become netcentric and more linked with our weapons systems, it is essential that our IA workforce be up to the task of securing our networks. I am proud to be on the cyber defense line with such a competent industry partner that understands the needs of the defense department and is willing to work with us to help accomplish this difficult task."

-MIKE KNIGHT, NAVAL NETWAR COMMAND



Why is SANS the best source for InfoSec training?

Thought Leader

SANS is the leading organization in computer security training. SANS provides intensive, immersion training designed to help you and your staff master the practical steps necessary for defending systems and networks against the most dangerous threats – the ones being actively exploited. The courses are full of important and immediately useful techniques that students can put to work as soon as they return to their offices. SANS courses were developed through a consensus process involving hundreds of administrators, security managers, and information security professionals. Our courses address both security fundamentals and the in-depth technical aspects of the most crucial areas of information security.

Best Instructors

SANS courses are taught in a classroom setting and by “SANS Certified Instructors.” The selection, training, and certification process to become a SANS faculty is time tested. Last year more than 90 people tried out for the SANS faculty, but only five new people were selected.

Significant Community Contributor

SANS develops, maintains, and makes available at no cost the largest collection of research documents about various aspects of information security. Additionally, SANS operates the Internet’s early warning system – the **Internet Storm Center**. At the heart of SANS are the many security practitioners in government agencies, corporations, and universities around the world who invest hundreds of hours each year in research and teaching to help the entire information security community. All this research and development activity helps to assure that SANS delivers the latest and greatest courseware available in the market today and produces the best instructors.

SANS courses are the best for information security training because:

- SANS training is full of important and immediately useful techniques that you can put to work as soon as you return to your office. That is the SANS Promise!
- SANS courses are developed through a consensus process involving hundreds of administrators, security managers, and information security professionals. Our courses address both security fundamentals and the in-depth technical aspects of the most crucial areas of information security.
- SANS features the best instructors and authors in the industry! To find the best faculty in the world SANS runs a continuous competition for instructors.
- SANS can deliver training to the DoD globally. We can deliver this training in one of many ways: **Global Events**, **OnSites**, and Web-based via **vLive!** & **On Demand**.
- SANS training supports a variety of 3rd party certifications, including those from CompTIA, CISA, & ISACA.

SANS training courses provide a solid foundation for the Global Information Assurance Certification (GIAC) which has over 22,000 security professionals who have already proven their skills and knowledge to meet our challenging standards. GIAC is unique in the field of information security certifications because it not only tests a candidate’s knowledge but also the candidate’s ability to put that knowledge into practice in the real world.



Where can I get SANS training?

SANS Global Events

Visit www.SANS.org for the nearest event location and course offerings.

SANS OnSite

Contact OnSite@sans.org today or visit www.sans.org/onsite to find out how you can bring SANS to your location for a private class.

SANS OnDemand

Online, self-paced training.

Contact 8570@sans.org today or visit www.sans.org/ondemand to learn more and get started.

Custom DoD "Blended Solution" Events

SANS can create a custom blended solutions for mid- to large-size classes. Such a solution can include any combination of live, interactive classes and online curriculum. Ask what we did for the Marines, Army, Navy, DLA, and PACOM.

Contact 8570@sans.org today or call Daryl Gilbertson at **678-714-5712**.

Other Options

- **SANS Mentor Program** (local, evening and smaller classes • www.sans.org/mentor)
- **SANS vLive!** (live virtual classroom instruction via webcast • www.sans.org/vlive)

For more information, please contact 8570@sans.org

View course descriptions and schedules at www.sans.org

Purchasing Options

Contract Payment Options and Vehicles

SANS accepts Government Purchase Cards, Credit Cards, Purchase Orders and Checks. We can also help you to purchase through other contract vehicles.

For more information, please contact 8570@sans.org.

SANS Voucher Credits

SANS Voucher Credits are a great solution for flexibility, cost savings, and value. It is perfect when you know that you will have a variety of IT Security training needs in the next 12 months, but have not decided who gets to go, what delivery format to use, or when to go. Voucher Credits are also perfect when you have discretionary training funds to spend for long-term professional development.

For more information, please contact Vouchers@sans.org or visit www.sans.org/vouchers.