SANS

DoD Directive (DoDD) 8570 & GIAC Certification

Date Updated: January 2014

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

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

www.sans.org/8570

SANS DoD Directive (DoDD) 8570 & GIAC Certification

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.

DoDD 8140 – The Future of DoDD 8570

DoDD 8570 will be converting to DoDD 8140 in 2013. More details on what will be changing as part of DoDD 8140 will be posted as it becomes available. Sections of DoDD 8140 will be based on the NICE Initiative at **http://csrc.nist.gov/nice/index.htm**

"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 McDougal, Raytheon

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.

SANS DoD Directive (DoDD) 8570 & GIAC Certification

DoD Baseline IA Certifications

TECH II

GSEC†
SEC401: SANS Security Essentials Bootcamp Style

Security+†

TECH III

GCIH†
SEC504: Hacker Techniques, Exploits, and Incident Handling

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

GCED†
SEC501: Advanced Security Essentials – Enterprise Defender

MGT I

GSLC†
MGT512: SANS Security Leadership Essentials For Managers

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

Computer Network Defense (CND) Certifications

CND ANALYST

GCIA†
SEC503: Intrusion Detection In-Depth

GCIH†
SEC504: Hacker Techniques, Exploits, and Incident Handling

CND INCIDENT RESPONDER

GCIH†
SEC504: Hacker Techniques, Exploits, and Incident Handling

GCFA†
FOR508: Advanced Computer Forensic Analysis and Incident Response

CND AUDITOR

GSNA†
AUD507: Auditing Networks, Perimeters, and Systems

Information Assurance System Architecture & Engineering (IASAE) 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.

SANS DoD Directive (DoDD) 8570 & GIAC Certification

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 40,000 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 mangers 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

- Go to The DoD8570 Information Assurance Workforce Improvement Program Office at **http://iase.disa.mil/eta/iawip**
- Call the Defense Information Assurance Program (DIAP) Office at **1-800-490-1643**
- Contact **8570@sans.org** or call Customer Support at **301-654-7267**.

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.

SANS DoD Directive (DoDD) 8570 & GIAC Certification

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, Pearson Vue. 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

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 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 updated multiple times throughout the year to keep up with the latest in the industry.
- SANS courses are written based on practical real world knowledge that you can apply as soon as you return to the office. That is the SANS courses.
- SANS courses are developed and taught by practitioners out in the field so you can be assured of instruction based on best practices in the marketplace.
- 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** and **OnDemand**.
- SANS training supports a variety of 3rd party certifications, including those from CompTIA, CISA, and ISACA.

SANS training courses provide a solid foundation for the Global Information Assurance Certification (GIAC) which has over 47,000 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.

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.

Live Classroom Training Formats

Multi-Course Training Events

Live instruction from SANS' top faculty, vendor showcase, bonus evening sessions, and networking with your peers

SANS Training Events are recognized as the best place in the world to get information security education, from intimate gatherings to SANS action-packed national events! Network with other information security professionals, hear world-class speakers, actively engage with providers of proven security solutions, and participate in challenges and contests. **www.sans.org/security-training/bylocation/index_all.php**

Select classes can be attended remotely via SANS Simulcast. **www.sans.org/simulcast**

Community SANS

Live Training in Your Local Region with Smaller Class Sizes

Community SANS offers the most popular SANS courses in your local community in a small classroom setting – most classes have fewer than 25 students. The course material is delivered just like it would be at a larger SANS event; but with SANS training brought to your community, you'll save money on tuition and travel. **www.sans.org/community_sans**

OnSite

Live Training at Your Office Location

With the SANS OnSite program you can bring a combination of high-quality content and world-recognized instructors to your location and realize significant savings in employee travel costs and on course fees for larger classes. **www.sans.org/onsite**

Mentor

Live Multi-Week Training with a Mentor

The SANS Mentor program offers the flexibility of live instruction with self-paced learning. Classes are conducted over the course of several weeks, much like a graduate level course. Students study on their own then work with the Mentor during class to discuss material, answer questions and work on exercises and labs such as Capture the Flag. **www.sans.org/mentor**

Summit

Live IT Security Summits and Training

SANS WhatWorks Summits are unique events that focus on the most current topics in computer security. User panels, debates, vendor demos, and short talks by industry experts help you get the most up-to-date security solutions in the least amount of time. **www.sans.org/summit**

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.

Online Training Formats

OnDemand

Self-Paced Online Classes, Learn at Your Convenience

OnDemand lets you access more than 25 SANS courses whenever and wherever you want. Each course gives you four months of access to our OnDemand e-learning platform, which includes a mix of presentation slides, video demonstrations, interactive labs, and assessment tests supported with audio of SANS' top instructors teaching the material. **www.sans.org/ondemand**

vLive

Live, Online Instruction from SANS' Top Instructors

SANS vLive allows you to attend live SANS courses from the convenience of your home or office. Log in at the scheduled times and join your instructor and classmates in an interactive virtual classroom. Classes typically meet two evenings a week for five or six weeks, perfect for professionals with busy lives. **www.sans.org/vlive**

Simulcast

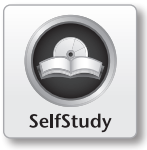
Attend a SANS Training Event Without Leaving Home

Event Simulcast allows you to attend a SANS training event without leaving home. Simply log in to a virtual classroom to see, hear, and participate in the class as it is being presented LIVE at the event. The Event Simulcast option is available for many classes taught at our largest training events. **www.sans.org/simulcast**

CyberCon

Live, Online Conference Featuring SANS' Top Instructors

Log into CyberCon, SANS' online conference, to experience a SANS training event without leaving home. Learn directly from SANS' top instructors, attend informative bonus sessions, and network with your peers at CyberCon! **www.sans.org/cybercon**



SelfStudy

Books and MP3 Files for Independent Learners

For the motivated student who enjoys working independently we offer the SANS SelfStudy program. Students receive SANS course books (and CDs when applicable) and online access to MP3 files of SANS' world-class instructors teaching the material. Study texts and listen to the lectures at your own convenience and pace. **www.sans.org/selfstudy**

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.