



**COURSE OVERVIEW HE0748(KO3)-4D**  
**Critical Infrastructure Security Force (CISF)**  
*(Level 1 & 2 Competencies)*

**Course Title**

Critical Infrastructure Security Force (CISF)  
*(Level 1 & 2 Competencies)*

**Course Date/Venue**

December 09-12, 2024/Fujairah Meeting Room,  
Grand Millennium Al Wahda Hotel, Abu Dhabi,  
UAE

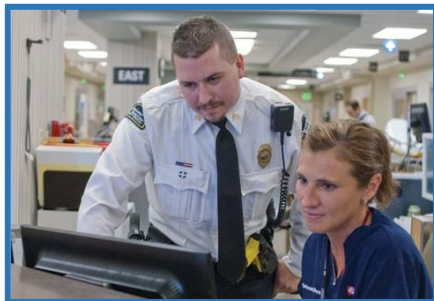
**Course Reference**

HE0748(KO3)-4D

**Course Duration/Credits**

Five days/2.4 CEUs/24 PDHs

**Course Description**



***This practical and highly-interactive course includes real-life case studies where participants will be engaged in a series of interactive small groups and class workshops.***



This course entrusted with very important and critical responsibilities of guarding the outer security cordon, as first line of defense, along with MOI's VOIPD personnel. The main responsibility involves checking all the personnel and vehicles at the main security cordon for suspected objects and at times engaging the intruders at this barrier and denying them entry into the main area of critical infrastructure such as refineries and other oil facilities.



In order to enable to perform his duties, he will be provided with special uniform and non-lethal weapons in addition to performing the tasks in line with other Security Men. This assignment carries additional responsibilities and dangerous exposures of tackling intruders and handling weapons. The job also involves special skills and tactics in tackling intruders.

At the completion of the course, each participant will be able to consistently demonstrate the competencies stated in the course competency objectives.



### **Course Competency Objectives**

Upon the successful completion of this course, each participant will be able to:-

- Apply and gain a comprehensive knowledge on critical infrastructure security force (CISF)
- Discuss the magnitude of the CISF entrusted with guarding the outer security cordon as first line of defence along with MOI's VOIPD personnel
- Recognize the responsibility of access control and apply extra precautions as well as deny entry into the main area of critical infrastructure in accordance with security threat protocols without exception
- Operate the physical security technology, tools and equipment assigned and communicate on access control breaches and malfunctions of alarm, security systems as required following appropriate procedures
- Use non-lethal weapons and confront intruders in a physical confrontation, subdue, restrain, and coordinate with local law enforcement agencies accordingly
- Monitor the checking of personnel, equipment, vehicles and goods to and from assigned area and facilities to ensure that only bona fide allowed access and exit from these facilities
- Maintain coordination with state installations security police and other state authorities in conducting physical searches of personnel, goods and vehicles and conduct non-intrusive inspections as needed.
- Liaise with the agencies in obtaining clearances and permission for bringing in photographic equipment, taking photographs of the facilities and for personnel required to take photographs
- Assist superiors in preparing special operations plans, including assembly of resources and task in the area of responsibility for patrol/drills or to target specific security breaches; commands/participates in the actual operation as directed
- Direct, supervise and control the activities of assigned personnel of Security Forces – CISF
- Formulate proposals for joint training and the development of doctrine for the deployment of CISF forces alongside VOIPD/MOI and for deployment in direct support of client's subsidiaries
- Develop and maintain security procedures and systems to protect company personnel, installations and property against undesirable activities or attempted activities such as theft, sabotage and ensures proper implementation of established security systems concerning CISF
- Act within the law and organizational policy and procedures including, personnel practices and guidelines.

### Exclusive Smart Training Kit - H-STK®



Participants of this course will receive the exclusive “Haward Smart Training Kit” (H-STK®). The H-STK® consists of a comprehensive set of technical content which includes **electronic version** of the course materials, sample video clips of the instructor’s actual lectures & practical sessions during the course conveniently saved in a **Tablet PC**.

### Who Should Attend

This course provides an overview of all significant aspects and considerations of critical infrastructure security force (CISF) for first line defense officers, security officers along with MOI’s VOIPD personnel.

### Training Methodology

This interactive training course includes the following training methodologies as a percentage of the total tuition hours:-

- 30% Lectures
- 20% Workshops & Work Presentations
- 30% Case Studies & Practical Exercises
- 20% Software, Simulators & Videos

In an unlikely event, the course instructor may modify the above training methodology before or during the course for technical reasons.

### Course Fee

**US\$ 4,500** per Delegate + **VAT**. This rate includes H-STK® (Haward Smart Training Kit), buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

### Accommodation

Accommodation is not included in the course fees. However, any accommodation required can be arranged at the time of booking.

**Course Certificate(s)**

Internationally recognized certificates will be issued to all participants of the course who completed a minimum of 80% of the total tuition hours.

**Certificate Accreditations**

Certificates are accredited by the following international accreditation organizations: -


- 

The International Accreditors for Continuing Education and Training (IACET - USA)

Haward Technology is an Authorized Training Provider by the International Accreditors for Continuing Education and Training (IACET), 2201 Cooperative Way, Suite 600, Herndon, VA 20171, USA. In obtaining this authority, Haward Technology has demonstrated that it complies with the **ANSI/IACET 2018-1 Standard** which is widely recognized as the standard of good practice internationally. As a result of our Authorized Provider membership status, Haward Technology is authorized to offer IACET CEUs for its programs that qualify under the **ANSI/IACET 2018-1 Standard**.

Haward Technology’s courses meet the professional certification and continuing education requirements for participants seeking **Continuing Education Units (CEUs)** in accordance with the rules & regulations of the International Accreditors for Continuing Education & Training (IACET). IACET is an international authority that evaluates programs according to strict, research-based criteria and guidelines. The CEU is an internationally accepted uniform unit of measurement in qualified courses of continuing education.

Haward Technology Middle East will award **2.4 CEUs** (Continuing Education Units) or **24 PDHs** (Professional Development Hours) for participants who completed the total tuition hours of this program. One CEU is equivalent to ten Professional Development Hours (PDHs) or ten contact hours of the participation in and completion of Haward Technology programs. A permanent record of a participant’s involvement and awarding of CEU will be maintained by Haward Technology. Haward Technology will provide a copy of the participant’s CEU and PDH Transcript of Records upon request.

- 

British Accreditation Council (BAC)

Haward Technology is accredited by the **British Accreditation Council** for **Independent Further and Higher Education** as an **International Centre**. BAC is the British accrediting body responsible for setting standards within independent further and higher education sector in the UK and overseas. As a BAC-accredited international centre, Haward Technology meets all of the international higher education criteria and standards set by BAC.





### **Course Instructor(s)**

This course will be conducted by the following instructor(s). However, we have the right to change the course instructor(s) prior to the course date and inform participants accordingly:



**Mr. Tony Bunce**, PgDip, BSc, RPA, CMIOSH, CRadP, NEBOSH, is an **Accredited Radiation Protection Adviser (RPA)** and a **Senior Environmental Consultant** with over **20 years** of extensive experience in **HAZOP & HAZAN** Analysis, Hazard Identification (**HAZID**), **ALARP** System, **Radiation Safety & Protection**, **Security Management**, **Security Operations Management**, **Investigation & Security Surveying**, **Security Crisis Management**, **Corporate Security Planning**, **Radioactive Waste Management**, **Radiation Protection Instrumentation**, **Nuclear & Radiological Safety**, **Nuclear Engineering**, **Safety Management System**, **Uranium & Plutonium Safe Handling**, **Contamination Control**, **Radiation Protection Design**, **Risk Assessment**, **Personal Protection Equipment**, **Dosimetry Review**, **Nuclear Weapon & Nuclear Reactor Accident Procedures**, **Personal Protective Equipment**, **Machinery & Work Equipment** and **Manual Handling**. Further, he is also well-versed in **ISO 14001:2004** (Environmental Management System), **AERMOD** Modeling, **Incident Reporting & Investigation**, **Cause Tree Analysis (CTA)**, **Fault Tree Analysis (FTA)**, **HSE** Emergency Planning, **Crisis Management**, **HSSE** Practices, **Emergency Response Plans** and **Emergency Preparedness**. He is currently the **Radiation Protection Advisor** of **IAEA (Austria)** wherein his in-charge of the design and commissioning of IAEA's new Nuclear Material Laboratory.

During Mr. Tony's career life, he held significant positions such as the **Radiation Protection Advisor**, **Radiation Protection Officer**, **Safety Adviser**, **Radiation Monitoring Specialist**, **Lead Safety Adviser** and **Health Physics Monitor** for international companies and agencies such as the International Atomic Energy Agency (**IAEA**), **Thorp Nuclear Processing Plant** and the **Nuclear Department of UK** just to name a few.

Mr. Bunce has a **Post Graduate Diploma** in **Radiation and Environmental Protection** from the **University of Surrey** and a **Bachelor** degree in **Environmental Risk Management** from the **University of Wales Institute Cardiff** in **UK** respectively. Further, he is a **Certified Instructor/Trainer**, a **Certified Internal Verifier/Assessor/Trainer** by the **Institute of Leadership & Management (ILM)**, an **Accredited Radiation Protection Adviser (RPA)** from the **RPA 2000 Board**, a **Qualified Radiological Protection Reviewer**, a Chartered Member of **IOSH (CMIOSH)**, a Chartered Radiological Protection Practitioner (**CRadP**), **Certified Radiation Safety Practice (Stage 1)** from **City and Guilds** and **NEBOSH Diploma** holder. He has further delivered numerous trainings, conferences, workshops and seminars globally.



**Course Program**

The following program is planned for this course. However, the course instructor(s) may modify this program before or during the course for technical reasons with no prior notice to participants. Nevertheless, the course objectives will always be met:

**Day 1: Monday, 9<sup>th</sup> of December 2024**

0730 – 0800	Registration & Coffee
0800 – 0815	Welcome & Introduction
0815 – 0830	<b>PRE-TEST</b>
0830 – 0900	<i>The Magnitude of the CISF is Entrusted with of Guarding the Outer Security Cardon, as First Line of Defense, along with MOI's VOIPD Personnel</i> <i>Denies Entry into the Main Area of Critical Infrastructure in Accordance with Security Threat Protocols without Exception</i>
0900 – 0915	Break
0915 – 1100	<i>The Magnitude of the CISF is Entrusted with of Guarding the Outer Security Cardon, as First Line of Defense, along with MOI's VOIPD Personnel (cont'd)</i> <i>Denies Entry into the Main Area of Critical Infrastructure in Accordance with Security Threat Protocols without Exception</i>
1100 – 1230	<b>How to Operate the Physical Security Technology, Tools &amp; Equipment Assigned</b> <i>Communicates on Access Control Breaches &amp; Malfunctions of Alarm, Security System as Required Following Appropriate Procedures</i>
1230 – 1245	Break
1245 – 1420	<b>How to Operate the Physical Security Technology, Tools &amp; Equipment Assigned (cont'd)</b> <i>Communicates on Access Control Breaches &amp; Malfunctions of Alarm, Security System as Required Following Appropriate Procedures</i>
1420 – 1430	<b>Recap</b>
1430	Lunch & End of Day One

**Day 2: Tuesday, 10<sup>th</sup> of December 2024**

0730 – 0900	<i>How to Use Non-Lethal Weapons &amp; How to Confront Intruders in a Physical Confrontation, Subdue, Restrain, &amp; Coordinate with Local Law Enforcement Agencies Accordingly</i>
0900 – 0915	Break
0915 – 1100	<i>Monitors the Checking of Personnel, Equipment, Vehicles &amp; Goods to &amp; from Assigned Area &amp; Facilitate to Ensure that Only Bona Fide Allowed Access &amp; Exit from these Facilities</i>
1100 – 1230	<i>Maintaining Coordination with State Installation Security Police &amp; Other State Authorities in Conducting Physical Searches of Personnel, Goods &amp; Vehicles &amp; Conducting Non-Intrusive Inspections as Needed</i> <i>Liases with Agencies in Obtaining Clearances &amp; Permissions for Bringing Photographic Equipment, Taking Photographs of the Facilities &amp; for Personnel Required to Take Photographs</i>
1230 – 1245	Break
1245 – 1420	<b>Assisting Superiors in Preparing Special Operation Plans</b> <i>Assembly of Resources &amp; Tasking in the Area of Responsibility for Patrol/Drills or to Target Specific Security Breaches</i>
1420 – 1430	<b>Recap</b>
1430	Lunch & End of Day Two





**Day 3: Wednesday, 11<sup>th</sup> of December 2024**

0730 – 0900	<i>Assisting Superiors in Preparing Special Operation Plans (cont'd) Commands / Participates in the Actual Operations as Directed</i>
0900 – 0915	<i>Break</i>
0915 – 1100	<i>Directing, Supervising &amp; Controlling the Activities of Assigned Personnel of Security Forces-CISF</i>
1100 – 1230	<i>Formulating Proposals for Joint Training &amp; the Development of Doctrine for Deployment of CISF Forces Alongside VOIPD/MOI &amp; for Deployment in Direct Support of Client's Subsidiaries</i>
1230 – 1245	<i>Break</i>
1245 – 1420	<i>Formulating Proposals for Joint Training &amp; the Development of Doctrine for Deployment of CISF Forces Alongside VOIPD/MOI &amp; for Deployment in Direct Support of Client's Subsidiaries (cont'd)</i>
1420 – 1430	<i>Recap</i>
1430	<i>Lunch &amp; End of Day Three</i>

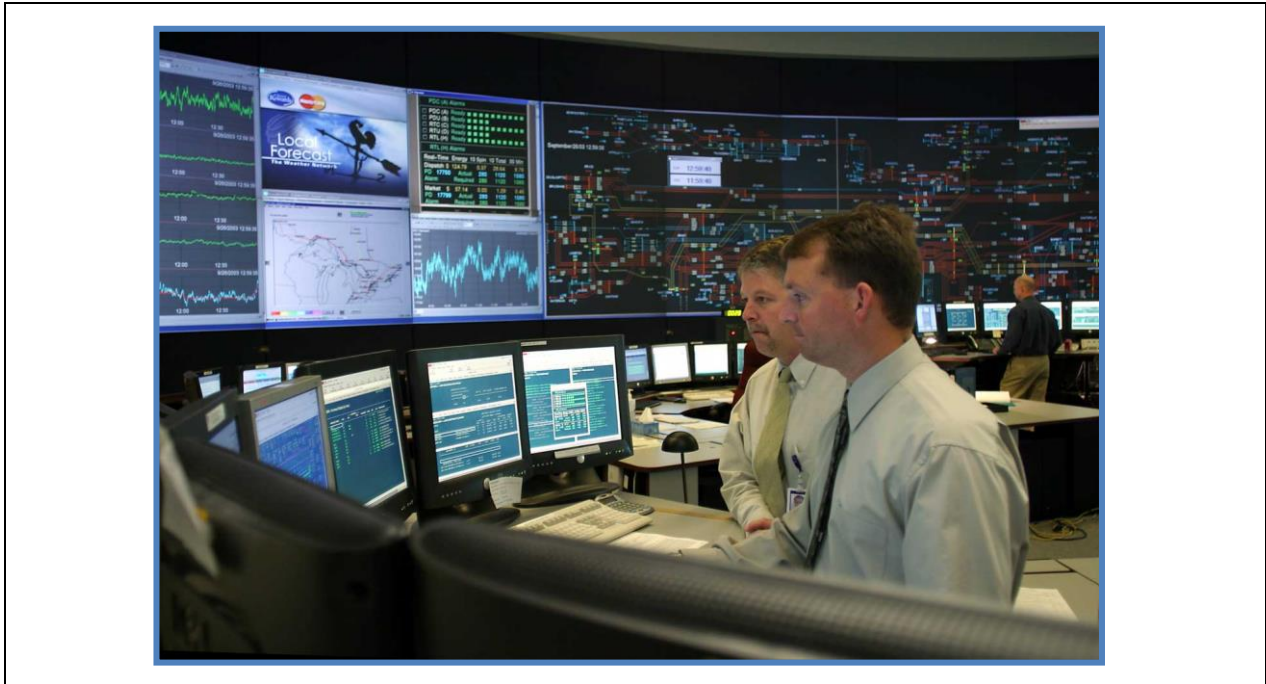
**Day 4: Thursday, 12<sup>th</sup> of December 2024**

0730 – 0930	<i>Developing &amp; Maintaining Security Procedures &amp; Systems to Protect Company Personnel, Installations &amp; Property Against Undesirable Activities such as Theft, Sabotage &amp; Ensures Proper Implementation of Established Security Systems Concerning CISF</i>
0930 – 0945	<i>Break</i>
0945 – 1100	<i>Developing &amp; Maintaining Security Procedures &amp; Systems to Protect Company Personnel, Installations &amp; Property Against Undesirable Activities such as Theft, Sabotage &amp; Ensures Proper Implementation of Established Security Systems Concerning CISF (cont'd)</i>
1100 – 1200	<i>Acts within the Law &amp; Organizational Policy &amp; Procedures Including, Personnel Practices &amp; Guidelines (cont'd)</i>
1200 – 1215	<i>Break</i>
1215 – 1345	<i>Acts within the Law &amp; Organizational Policy &amp; Procedures Including, Personnel Practices &amp; Guidelines</i>
1345 – 1400	<i>Course Conclusion</i>
1400 – 1415	<i>POST-TEST</i>
1415 – 1430	<i>Presentation of Course Certificates</i>
1430	<i>Lunch &amp; End of Course</i>



**Practical Sessions (Case Studies)**

This practical and highly-interactive course includes real-life case studies and exercises:-



**Course Coordinator**

Mari Nakintu, Tel: +971 2 30 91 714, Email: [mari1@haward.org](mailto:mari1@haward.org)