



Projects Plan

Ministry of Interior
State of Qatar



وزارة الداخلية
Ministry of Interior
دولة قطر • State of Qatar



وزارة الداخلية
Ministry of Interior

دولة قطر • State of Qatar



Introduction

Under the kind patronage of H.H. Sheikh Tamim Bin Hamad Al Thani Amir of the State of Qatar, the 15th edition of the International Exhibition for Homeland Security and Civil Defence, Milipol Qatar Exhibition will be held on 29th to 31st October 2024 in Doha - State of Qatar.

The 15th edition of Milipol Qatar Exhibition, which is recognized internationally as one of the most prominent specialized security exhibitions, provides an ideal opportunity to get acquainted with the new technology in security field. It also meets a large part of the growing security needs of the State of Qatar and the Middle East. Milipol Qatar provides access to security markets in the entire region and enables key international industry players to meet in a fast-developing environment with medium-to long-term economic and strategic projects.

This generous patronage is in line with Qatar National Vision 2030 which was led on social foundation conveying the importance to create a society enjoying peace and prosperity, expressing the kind support of His Highness to the international efforts seeking peace and security for international community in a time when the world is witnessing an escalation of problems threatening the world peace.

On this occasion, we designed this booklet to highlight some projects of the Ministry of Interior departments and their security requirements for future projects. Conveying with the developments witnessed by the State of Qatar, the role of Ministry of Interior and its departments is getting bigger in the field of maintaining security and stability to meet with the requirements of comprehensive renaissance and development in the country through proper supply of security devices, equipments, systems and widening the scope of rendered services for the public according to the creative security strategic plans that comprise of requirements of the present and the future.

Milipol
QATAR 2024

11th Edition

SAVE THE DATE

29-31 October 2024
Doha-Qatar

International Event For
Homeland Security & Civil Defence

Milipol Qatar 2024



وزارة الداخلية
Ministry of Interior
دولة قطر • State of Qatar

milipolqatar.com

[milipolqatar](https://www.youtube.com/milipolqatar) [f](https://www.facebook.com/milipolqatar) [X](https://www.x.com/milipolqatar) [in](https://www.instagram.com/milipolqatar) [in](https://www.linkedin.com/company/milipolqatar) [v](https://www.youtube.com/milipolqatar)



وزارة الداخلية
Ministry of Interior
دولة قطر ♦ State of Qatar

Ministry of Interior Projects



وزارة الداخلية
Ministry of Interior
دولة قطر • State of Qatar



General Directorate of Coasts and Borders Security

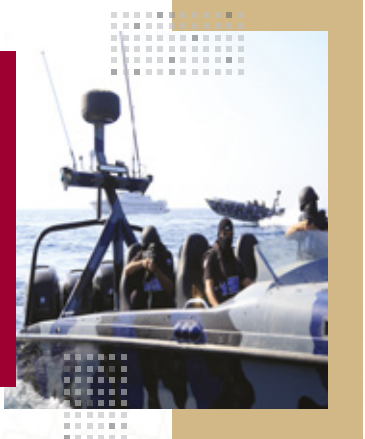
We would like to inform you that the unified coastal radar system of the General Directorate of Coast and Border Security has been developed. The FURUNO 2228 radars are operated and activated in all coastal towers in north, south, east and west of the state.

Now all the radars are activated by the radar operator located in the control room of the tower inside the outer centers.

Based on what has been stated, we recommend the establishment of a unified control room for the management of the coastal radar system, which is similar to the (Dir'a) system, so that the control rooms of this system are located within the Al Daayen Marine Base.

Control rooms are designed inside the operations building so that from this room the coastal radars are controlled remotely to facilitate the monitoring process and the work of the radar operators. With the control room inside the operations building, we will notice the ease and speed in making decisions to confront any potential target. We will also avoid the problem of radar operators access to and from outside centres and the problem of follow-up preparation, meals and accommodation.

Finally, we will have established a modern and upgraded control room with the best technology and means of communication to follow up and monitor the objectives found in the territorial waters of North, South, East and West of the State from a special control room in the General Directorate of Coast and Border Security only at Al-Daayen Marine Base.



Marine fleet maintenance department plan

1. Purchase of 40 routine patrol boats, which are no longer than 40 feet in length, equipped with two or three outboard engines, and to take into consideration the tasks required by this boat is routine patrolling on the coast.
2. Purchase of 6 security boats (patrol boat). It is used to secure important personalities and facilities, and is characterized by its closed and air conditioned form.
3. Purchase of 6 medium range boats, which are boats that withstand sever weather conditions and are used in open areas and characterized by speed and stability.
4. Purchase of 10 patrol boats for special missions, which are used for pursuits and special missions, and characterized by high speeds and advanced surveillance systems.



National Command Centre (NCC)

- Developing the Command and Control systems related to emergency service.
- Developing all the Geographical information systems.
- Developing the unified Integrated communication system handling the (999) emergency calls.
- Developing the Automatic vehicle location tracking system and its used devices.
- Developing the Command and Control devices related to operations rooms.
- Developing the Command and control vehicle.



General Directorate of Information Systems

1. MOI Asset Management Project

Asset Management software systems aim at using - in an optimal way - MOI's assets by:

- Identifying and following-up on such assets.
- Maintaining assets.
- Knowing current assets' market value.
- Date of exclusion hence avoiding overstock of unwanted assets or purchasing assets that are already available in other locations.
- The system of placing under electronic surveillance using the electronic bracelet is considered a modern technique to preserve the requirements of judicial control, as it is one of the alternatives for implementing short-term freedom deprivation penalties.

2. Electronic Bracelet

Objectives of electronic bracelet:

- Modern alternatives for implementing deprivation penalties.
- Prevent social isolation.
- Alleviation for convicts in simple cases.
- Prison overcrowding.
- Reduce the cost.



3. Data Loss Prevention (DLP)

This project aims to classify regulated, confidential and business critical data and identifies violations of policies defined by MOI or within a predefined policy pack.

Goals:-

- Protects sensitive information across emails, web, and endpoint platforms.
- Leverages machine learning for effective data identification and protection.
- Integrates seamlessly with existing on-premises and cloud environments.
- Supports compliance with data privacy regulations, ensuring regulatory conformity.
- Promotes the trust and reputation of our organization by preventing data breaches.
- Utilizes advanced policy enforcement for comprehensive data loss prevention.
- Facilitates incident management, enabling rapid response to potential threats.



4. VDI

VDI, refers to the process of running a user desktop inside a virtual machine that lives on a server in the datacenter or a server farm. It's a powerful form of desktop virtualization because it enables fully personalized desktops for each user with all the security and simplicity of centralized management.

Goals:-

- Technology Benefits:
 - Simplify management and improve control.
 - Improved security, mitigates threat of data loss.
 - Massively reduced upgrade costs and timescales (up to 50%).
 - Extend business continuity and disaster recovery to desktops.
- Business Benefits:
 - User mobility across sites/departments.
 - Deployment of new sites/offices cheaper and quicker.
 - Desktop MADC effort significantly reduced.
 - Consistent and personalize end user experience.

5. Data Center Security

- Complete server protection, monitoring, and workload micro-segmentation for private cloud and physical on-premises data center environments.
- Block zero-day exploits with application whitelisting, granular intrusion prevention, and real-time file integrity monitoring (RT-FIM)



6. MOI Centralized Data Protection/Anti Ransomware Solution

- Provides business with unified data management platform as the last line of defence against the cyber/ransomware attacks. Enhances the data protection capability of MOI to meet the modern-day needs.
- Creates immutable copy, so that in case of an attack, there is a secure copy to recover your data from.
- Introduces Air-gap mechanism, physically isolating the vaulted copies of the clean data.
- Multiple point-in-time copies of data are maintained as failsafe and/or for forensics purposes
- Retention lock adds another layer of protection from both internal and external threats.
- Data validation capabilities to detect threats
- Recovery data is maintained on hybrid storage, substantially speeding up the time for data recovery processes
- Multifactor Authentication and zero trust access controls add extra layer of data protection.
- Immutable data backup copies.

7. Extended Detection and Response (XDR)

This project is a consolidation of tools and data that provides extended visibility, analysis, and response across endpoints, workloads, users, and networks.

XDR unifies endpoint and workload security capabilities with critical visibility into the network and cloud—reducing blind spots, detecting threats faster, and automating remediation via authoritative context across these domains.

Goals:-

- Integrates multiple security products for an improved incident detection and response, a critical need in large government networks to quickly identify and mitigate threats.
- Collects and correlates data from various sources, such as EPP and network security, providing a more complete view of potential security incidents.
- Improves threat detection and response speed compared to standalone security products, reducing the potential impact of cyber-attacks on government services.
- Offers an additional layer of protection by simplifying security operations and increasing overall protection.
- Provides a holistic view of the threat landscape, crucial for the proactive defense of government systems.



8. Network Detection and Response (NDR)

This project provides solution that continuously monitors MOI network to detect cyber threats & anomalous behavior using non-signature-based tools or techniques and responds to these threats via native capabilities or by integrating with other cybersecurity tools/solutions.

Goals:-

- Built on the open-source network security monitor Zeek.
- Converts raw network traffic into detailed logs, extracted files, and actionable security insights, helping detect potential intrusions or unauthorized activities in government networks.
- Enhances threat detection and accelerates threat-hunting capabilities, critical for identifying and responding to threats to government systems.
- Facilitates faster incident response and forensics, essential for maintaining the security and integrity of government digital infrastructure.
- Provides an additional layer of defense through in-depth network visibility and threat detection.



9. Identity Access Management (IAM)

This project aims at enabling the right individuals to access the right resources at the right times and for the right reasons. It addresses the need to ensure appropriate access to MOI resources across increasingly heterogeneous technology environments and to meet increasingly rigorous compliance requirements.

Goals:-

- Enables robust control over access permissions, safeguarding against internal breaches.
- Automates user-access management, saving valuable time and resources.
- Promotes transparency and accountability across systems.
- Ensures compliance with access control regulations.
- Provides comprehensive access reporting for audit purposes.
- Facilitates governance of both on-premises and cloud access.
- Implements policy-based control to maintain granular access rights.



This project ensures that the right people and job roles in your organization (identities) can access the tools they need to do their jobs. Identity management and access systems enable your organization to manage employee apps without logging into each app as an administrator.

Goals:-

- Implements robust, policy-based control over user access to applications, limiting the potential for insider threats in government departments.
- Provides automated management for complex user-access scenarios, streamlining operations within government entities.
- Features comprehensive access reporting, enhancing visibility and accountability across systems.
- Reduces risk associated with inappropriate access rights, a critical factor in maintaining the confidentiality and integrity of government data.
- Supports compliance with access control regulations and standards that are often essential for government agencies.

General Directorate of Civil Defence

1. Setting up of a specialized laboratory for testing safety and security materials, equipment and systems for the Civil Defense.

In view of the vital and important role that the Civil Defense plays in protecting lives and properties, there must be a specialized scientific laboratory of high technology, equipped with the latest means and modern technology in order to carry out the tasks assigned to it efficiently and accurately.

2. Electronic System for following up the maintenance procedures of the fire prevention systems.

Developing an electronic system that simplifies follow up task of the firefighting procedures and its maintenance and connecting it with the General Directorate of Civil Defense, as the electronic system will contribute to confirm the sustainability of the systems and its continuity at all establishments that come under the provisions of the civil defense in the country and the primary objective of the General Directorate is to protect the lives and properties.



General Directorate of Industrial Security

Details of the important projects of the General Directorate of Industrial Security and procurement of security systems to be implemented during the next three years are:

1. Counter drone system for critical oil and gas facilities at Ras Laffan Industrial City, Mesaied Industrial City, Vital establishments at Dukhan Operations and Halul Iceland.
2. Surveillance system for the critical hydrocarbon transmission and distribution pipelines.
3. Replacing/ Updating security surveillance systems for Halul Iceland.
4. Replacing the Analog cameras with IP cameras and updating security surveillance system at Ras Laffan Industrial City.



General Directorate of Traffic

1. Control and Surveillance room at the headquarters of the Licensing Affairs Department in the General Directorate of Traffic, Madinah Khalifa.
2. Smart cars for the driving test to evaluate the new trainees and determine whether they passed the driving test or not.

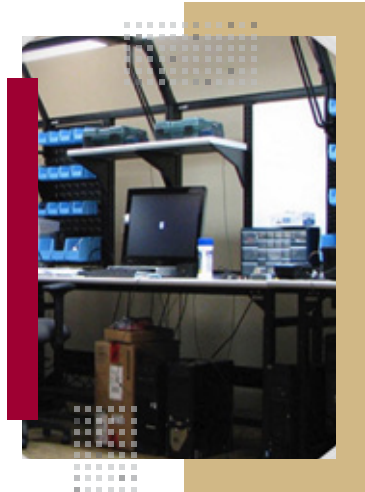


General Directorate of Criminal Investigation

The digital laboratory development project

Introduction:

The digital laboratory development project aims to develop and equip the department with the cutting-edge technologies in digital forensics, attract qualified human resources and obtain ISO accreditation for the digital evidence laboratory. The project is expected to increase the processing speed of the digital evidence, develop and construct the laboratory building in accordance with international standards, increase the absorptive capacity to cope with the increase in the volume of communications, and raise the efficiency of laboratory testing work in accordance with international standards. The project also aims to create a reliable process management system to ensure Chain of Custody reliability at the regional and global levels.



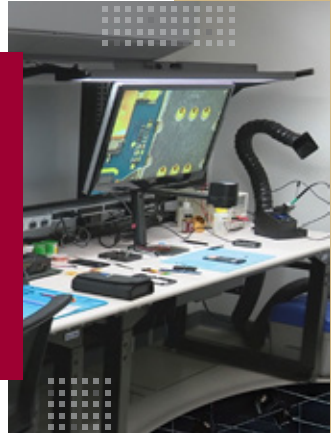
Main objectives:

The digital evidence laboratory development project aims to develop and equip it. The project was initiated due to the increasing reliance on the analysis of digital evidence in various criminal investigations and not only in cybercrimes, which requires the use of advanced tools and techniques to analyze digital devices and data.

This project aims to provide the Digital Evidence Laboratory with the cutting-edge tools, techniques and trained personnel to conduct an effective digital forensic analysis. The project will help speed up the processing of digital evidence, allowing for the expansion of digital inspections to include variety of evidences types like internet-connected devices, drones, and chip-off examinations.

The project also recognizes the importance of qualified personnel in analyzing digital evidence. Therefore, the project will focus on training and qualifying the current employees, in addition to attracting qualified employees with experience in this field. In sum, the project aims to:

1. Enhance equipment, systems, and programs capabilities.
2. Qualifying Investigators capabilities in the digital evidence laboratory and attracting qualified personnel with experience in the field.
3. Establish and implement a system for managing operations and the digital evidence's chain of custody.
4. ISO accreditation: As an inevitable result of the development processes, the project aims to obtain ISO accreditation for Forensics laboratories - Digital Evidence Laboratory. ISO accreditation will ensure that the digital forensics laboratory adheres to international standards and best practices in the field of digital forensic examination.



Open Source Intelligence (OSINT) and Social Media Intelligence (SOCMINT)

1. Introduction:

The purpose of this project is to establish an Open Source Intelligence (OSINT) and Social Media Intelligence (SOCMINT) operation focused on monitoring and detecting unlawful activities in Qatar's cyberspace. The operation will utilize a comprehensive SOC-like environment and cutting-edge technologies to provide real-time monitoring, analysis, and reporting of potential cybercrimes. By leveraging experienced professionals and advanced tools, this operation aims to identify threats and neutralize them before they can cause harm. The key features and benefits of the operation are outlined below.



2. Key Objectives:

The project has the following key objectives:

- a. **Efficiency:** Reduce the time and effort required for manual data collection and analysis, enabling the team to focus on proactive threat detection and response.
- b. **Quick and Smooth Access:** Establish a centralized hub (OSINT Room) that enables quick and seamless access to required data from various online sources, including the dark web processes at various levels within the department.
- c. **Enhanced Investigation and Decision-making:** Accelerate and improve the electronic search, investigation, and decision-making processes at various levels within the department.
- d. **Insights and Perceptions:** Gain clear insights and perceptions on various topics and issues by harnessing the data available on social media platforms.

- e. **Proactive Database:** Build a proactive database that serves as a foundation for electronic search and investigation operations, allowing for the identification of crime trends and the discovery of perpetrator identities.
- f. **Link Analysis:** Uncover hidden links between various crimes, facilitating a more comprehensive understanding of the cyber criminal landscape.
- g. **Artificial Intelligence (AI) Techniques:** Utilize artificial intelligence and deep learning techniques to enhance data analysis and derive the best possible results.
- h. **Future Crime Trends:** Leverage collected data to determine future crime trends and develop proactive measures accordingly.

3. SOC-like Environment and Setup

The OSINT/SOCMINT operation will be designed to resemble a Security Operations Center (SOC) environment, equipped with advanced tools and technologies.

4. Conclusion

The OSINT/SOCMINT operation will significantly enhance the department's ability to proactively and effectively respond to cybercrime threats in Qatar's cyberspace. By reducing manual efforts, improving data accessibility, and leveraging advanced technologies, the operation will enable the team to gain valuable insights, determine crime trends, reveal hidden links between crimes, and effectively utilize machine learning and artificial intelligence techniques. The project's outcomes will establish a solid foundation for future investigations, contributing to the prevention and mitigation of unlawful activities online.

ID Screen 60 for Travel

Multi-Biometric Tablet For Mobile Forces

At borders, mobile forces operate in challenging environments. They must facilitate smooth clearance processes while simultaneously acting on possible threats.

Main functions of a multi-application biometric tablet

1- Enrollment:-

- Demographic data.
- Fingerprints (10 fingers).
- Portrait.
- Signature.
- Photos of administrative/ID documents.



2 – ID document check:-

- Reads multiple ID documents.
- ID cards (contact, contactless, barcode).
- Driver’s licenses.
- ePassports.
- ID check using portrait or fingerprints.

3 – Identification:-

- Remote 1:N search via an ABIS (fingerprints, portrait).
- On-device 1:N search against a local watch.



Face Recognition

Facial recognition is a computer vision technique that scans and recognizes human faces from images or reality. It compares a human face against a computerized blueprint to attest.



Car Inspection Device

Ensure the data obtained during an acquisition contains the expected types of information. Determine if the data present relates to an investigation and verify key information that will be used as evidence.



SIS 3

Systems are capable of displaying multiple sound spectrograms, adjusting the time alignment and frequency ranges and taking detailed numeric measurements of the displayed sounds with these advances in technology.



Digital Forensics

- Case & workflow management with proactive warning & messaging capabilities.
- Automatic expertise report generation and dynamic statistical reports.
- Staff & equipment monitoring with operational dashboards and tracing capabilities.





Ministry of Interior

General Directorate of Traffic



 www.moi.gov.qa

   @moi_qatar |  moigovqatar |  moigovqa

Metrash2

To activate Metrash2

92992

Know our services
on Smartphones

Traffic services

Residence Services

Entry permit services

General Services












Milipol Qatar

29-31
October | **2024**

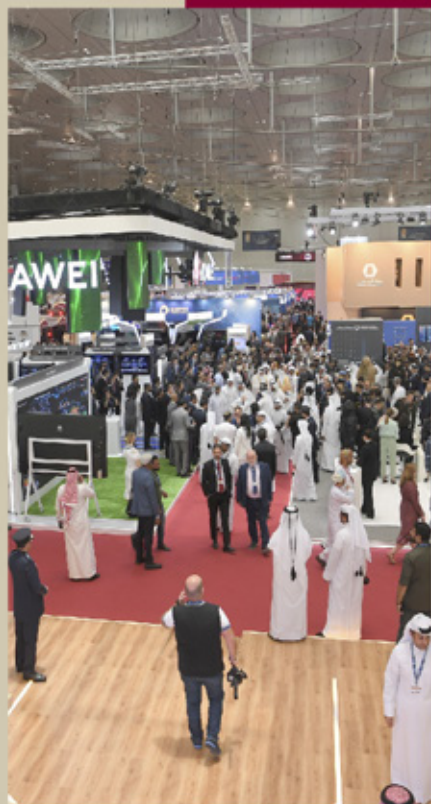
Doha-Qatar

 milipolqatar     

 www.milipolqatar.com

Milipol

Qatar Exhibition
2024

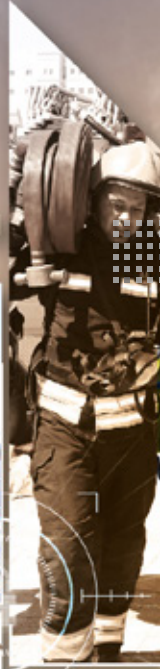




International Event For Homeland Security & Civil Defence



**Milipol
Qatar
2024**



*With Compliments of Milipol Qatar Committee
State of Qatar*