Karni Security Plan

There is a consensus that the Karni crossing security deficiencies are mostly related to personnel and process. While infrastructure and equipment improvements are needed, the immediate focus should be to address the personnel and process issues. Following are the main elements of the plan to enhance security at Karni:

- The Palestinian leadership is committed to enhancing security at Karni, with the assistance of Lt. Gen. Dayton's team and the international community.

- The plan envisages as an immediate measure complete control over all access to the Restricted Area of the crossing.

- The plan also requires bringing all security functions under the leadership of the PG to ensure the security process is adhered to in full

- Training, acquiring equipment, and upgrading infrastructure are important elements in the plan, and are phased throughout the implementation of the plan.

Following is the plan in detail:

1.   PERSONNEL

Immediate

- Presidential Guard Task Force (PGTF) will be deployed to oversee operations at the perimeter (conducted by NSF) and all operations inside the crossing (PSO, staff, workers) similar to the arrangements at Rafah.
- The estimated size of the force is between approximately 200-400 personnel. The exact number would depend on the number of shifts and hours of operation.

Medium Term

- All persons (Security Personnel, Staff/Workers, Drivers, Traders) that had previous access to the Restricted Area who fail the improved vetting process would be removed from the Final List granting access to the Restricted Area (see process below).

Long Term

- Complete replacement of existing security personnel by a newly trained force trained in facilities in Jordan.
- The training for around 100 personnel per month will be up to international standards and specifically tailored to the requirements of Karni (module for cargo inspection training).

- All persons in the Final List of people granted access to the Restricted Area (Security Personnel, Staff/Workers, Drivers, Traders) will be issued swipe card/smart card and readers will be installed in the various sectors of the crossing so that only persons that are authorised to be in a specific sector would be allowed in.

- The list of persons granted access to the Restricted Area may be submitted to Israel, as was the case in Rafah.

2.   PROCESS

Immediate

- A list (Names + ID number) of all persons (Security Personnel, Staff/Workers, Drivers, Traders) currently granted access to the Restricted Area will be supplied.
- All current workers will wear distinctive uniforms identifying their functions and area(s) of operation.
- All persons with access to the Restricted Area (Security Personnel, Staff/Workers, Drivers, Traders) will wear visible badges to verify identity and function. Visitors to the Restricted Area will be subject to an on-site security check. If granted access, they will wear a distinctive badge that specifies their level of access and indicates that they must be accompanied by a staff member at all times.
- No person will be allowed entry into the Restricted Area without being checked for weapons and explosives.

Medium Term

- A Designated Party (DP) will adopt and implement a rigorous vetting process as follows:
  - The DP will review the database of all persons (Security Personnel, Staff/Workers, Drivers, Traders) with access to the Restricted Area according to the adopted vetting process.
  - The DP will decide whether the person will be:
    - Confirmed access (confirmed on the Final List)
    - Checked further before they get confirmed
    - Denied access (removed from the Final List)

  - The DP will then check the names and IDs of those who are not currently in the database using the adopted vetting process before adding them to the Final List.
  - The DP will conduct a special check for Security personnel.
  - The adopted vetting process will include:
    - input from Intelligence, Preventive Security, and Police
    - periodic checks
    - random checks

- ▪ real-time feed of information from these agencies to the operations room

Long Term

- Implement Risk Management System:
  - o Devise procedures detailing the Risk Management System.
    - ▪ System assigns risk categories (green, yellow, red) , and implement checks on all high risk (red), some medium risk (yellow)
    - ▪ Additional random checks driven by the system (i.e. no discretion to officers)
  - o Secure infrastructure (hardware, software, equipment, personnel) to implement the system
  - o Gather full information on shipments ahead of time of arrival at the crossing.
  - o Implement Trade Chain Security Programme: work with businesses to secure shipments from factory floor to the crossing.

3. INFRASTRUCTURE AND EQUIPMENT

Current infrastructure, although very basic, can provide for a manageable level of security in the immediate term if coupled with improvements in process and personnel.

Immediate
- o Electronically controlled heavy duty gates code-operated
- o Concrete blocks to prevent bypassing the gates
- o Trained dogs for explosives detection
- o Explosives detection equipment (Hand-held)
- o Metal detectors (Hand-held)
- o Computers/Laptops + software for handling the list of people granted access
- o Operations room (basic for coordinating external perimeter and internal operations)
  - Wireless communication
  - Land lines
  - Connection to Intelligence, Preventive Security, and Police
- o Adequate living facilities for PGTF (incld. barracks)
- o Sufficient weapons and ammunition for PGTF to perform its duties

Medium Term
- o Cameras connected to CCTV system
- o Operations room (fully equipped)
- o Lighting
- o Fence/ Wall improvements

Long Term
- o Reconfiguration and modernisation of the whole terminal (including upgrading fence, improve docking)

4.   SYSTEM INTEGRITY

Medium Term

Queuing and scheduling
- Transparent, system-driven process
- Rules to be developed together with the private sector.
- All information (rules, schedule, fees, exceptions, updates) to be published on website. Any modification would have a record of whom, when, and why that was carried out.

Addressing dual loyalties
- Provide appropriate remuneration for personnel including social benefits such as health care and housing facilities, and/or incentive payments (bonuses, rewards, etc.).

- Devise and issue Code of Conduct with clear sanctions; personnel who violate rules lose their job or pay penalty, users lose access privilege.

Long Term

Addressing dual loyalties
- Internal and external auditing.
- Appoint an Ombudsman to oversee operations and investigate complaints
- Strategic segregation of functions; rotation of assignments and random allocation of examinations among officers. In certain cases, regular relocation of staff.
- Administration should foster an open and transparent relationship with Customs brokers and with the relevant sectors of the business community, through such means as liaison committees.