

WORKBOOK 14.1: SECURITY INSPECTION AND VALIDATION (SIV) PROGRAM DIRECTIVE



Purpose: To present a simplified example of a security inspection and validation program directive

Security Inspection and Validation Program Directive Example

Department of Ministry	Order 346.2b
Introduction	
This standard operating procedure was developed to provide guidance to SIV teams, vulnerability analysis teams, and other related security audit groups who are charged with the responsibility to ensure that critical infrastructure facilities possess effective and efficient security measures.	
Reference List	
The following references were used in the creation of this standard operating procedure:	
<ul style="list-style-type: none"> ▪ National Firearms Qualification Directive 100.1 — States the requirements for law enforcement officer and security force qualifications. ▪ Storage of Classified Documents Guide 200.0 — States the types of containers required to store classified information. ▪ Physical Fitness Standards for Security Force Order 110.0 — States the physical fitness requirements that must be maintained by a security force member. 	
Definitions: The following list of definitions apply to this standard operating procedure:	
CCTV	Closed-circuit television; used to monitor specific locations through the use of cameras and a television monitor.
Security force member	An authorized member of the critical infrastructure's security force, who has achieved at least 150 hours of training to include firearms, defensive tactics, driving and patrol procedures, from a certified training facility.
SIV	Security inspection and validation

Concept of Operations:	
The security inspection and validation should be conducted on an annual basis for every critical infrastructure within the nation.	
The following directives apply to conducting such activities:	
<ul style="list-style-type: none"> ▪ A qualified team of experts will conduct each security inspection and validation. 	
<ul style="list-style-type: none"> ▪ Inspections will be coordinated with the critical infrastructure security management team. 	
<ul style="list-style-type: none"> ▪ The security inspection and validation team will conduct a pre-inspection briefing with the critical infrastructure facility management prior to the inspection. Once the on-site visit is completed, they will conduct an out-briefing with the critical infrastructure facility management to discuss any observations or findings. 	
<ul style="list-style-type: none"> ▪ The security inspection and validation team will ensure that all documentation is submitted accurately and in a timely manner. 	
Responsibilities and Authorities:	
SIV Program Director	Responsible for oversight of the security inspection and validation team program and all managerial elements of the program and assigned personnel.
SIV Team Leader	Responsible for leading security inspection and validation teams through the use of qualified experts, and coordinating on-site inspections as well as validating the observations and findings documented during the inspection.
Critical Infrastructure Security Manager	Responsible for developing a corrective action plan that describes the observations and findings from the inspection, which includes recommendations on how deficiencies will be addressed.