The President’s Commission on Critical Infrastructure Protection (PCCIP) provided the outlines of a strategy for a layered defense that included activities in policy formulation; prevention and mitigation; information sharing and operational warning; counteraction (incident management); and response, restoration, and reconstitution (consequence management).

Policy formulation activities include

- assess national risk;
- integrate public and private sector perspectives;
- propose national objectives and develop strategies;
- propose and promote (new) legislation;
- assess and promote (new) regulations;
- influence private sector investments;
- prepare, recommend, and promote budget;
- manage and enforce implementation;
- shape the international environment; and
- issue the national policy.

Prevention and mitigation activities include
• provide effective education and awareness;
• set standards, certifications, and best practices;
• assess vulnerabilities and risks of system components;
• research advanced techniques and develop new technologies;
• negotiate funding;
• acquire the resources for protecting systems; and
• manage operations consistent with best practices.

Information sharing and operational warning activities include
• share information;
• analyze information and prepare threat advisories; and
• disseminate warnings.

Counteraction (incident management) activities include
• develop incident management policy and plan operations;
• deter, halt, or minimize an attack;
• implement defensive actions;
• punish perpetrators during or after an attack;
• control misinformation and manage perceptions; and
• coordinate incident and consequence management.

Response, restoration, and reconstitution (consequence management) activities include
• plan for the response to consequences;
• manage the response to consequences;
• plan for restoration and reconstitution; and
• manage restoration and reconstitution.