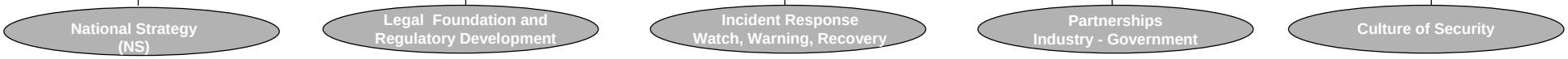
Cyber Security and Critical Infrastructure Protection

Model National Plan



POLICY: *Protection of critical national information infrastructures and cyberspace are essential to national security and a nation's economic well-being. Critical national information infrastructures and cyberspace are interconnected across industry sectors and national borders. The protection of these infrastructures and cyberspace requires coordinated national action related to the prevention, preparation, response, and recovery from an incident on the part of government authorities at the national, state and local levels; the private sector; and citizens/users; and cooperation and coordination with international Partners.*

1 - Goals:

NS 1.1 Create awareness at policy level of cyber/Critical Information Infrastructure Protection (CIIP) issues and need for national action and international cooperation.
NS 1.2 Develop a national strategy to protect national critical information infrastructures and cyberspace from all-hazards (cyber and physical) incidents.
NS 1.3 Join international efforts to coordinate activities related to the prevention, preparation, response, and recovery from incidents.

2 - Actions:

NS 2.1 Undertake policy level discussions with major players and key decision makers with regard to threats and vulnerabilities and the need for national action.
NS 2.2 Identify lead institution for national effort and lead institutions for each aspect of the national strategy.
NS 2.3 Identify points of contact within government ministries, state and local government, and the private sector.
NS 2.4 Identify roles, responsibilities and cooperative arrangements for and among all participants.
NS 2.5 Establish mechanisms for cooperation among government and private sector entities at the national level.
NS 2.6 Join international information sharing and assistance mechanisms.
NS 2.7 Assess and conduct periodic reassessments of the current state of cyber security and CIP, and develop program priorities.
NS 2.8 Identify training requirements and need for technical exchanges.

POLICY: *The protection of critical national information infrastructures and cyberspace requires the updating criminal law, procedures and policy to address and respond to cybersecurity and cybercrime.*

1 - Goals:

LR 1.1 Enact and enforce a comprehensive set of laws relating to cybersecurity and cybercrime in accordance with the provisions of international legal instruments and the Council of Europe's Cyber Crime Convention (2001).

2 - Actions:

LR 2.1 Assess the current legal authorities for adequacy.
LR 2.2 Draft and adopt substantive, procedural and mutual assistance laws and policies to address computer-related crime.
LR 2.3 Establish or identify national cybercrime units.
LR 2.4 Develop cooperative relationships with other elements of the national cyber security infrastructure and the private sector.
LR 2.5 Develop understanding of cyber crime issues in judiciary and legislative branches of government.
LR 2.6 Participate in the 24X7 Cybercrime Point of Contact Network.

POLICY: *Maintain an organization to serve as a focal point for securing cyberspace and the protection of critical national information infrastructures, whose mission includes watch, warning, response and recovery efforts and the facilitation of interactions and collaboration between and among government entities at the national, state and local levels; the private sector; academia; and internationally.*

1 - Goals:

IR 1.1 Develop a national cyberspace security response system with effective organizations to prevent, predict, detect, respond to and recover from cyber incidents.
IR 1.2 Develop national cyberspace threat and vulnerability reduction program in coordination with the intelligence and law enforcement communities.
IR 1.3 Develop national cyberspace security awareness and training program.
IR 1.4 Develop procedures and capabilities to secure government computer systems and networks.
IR 1.5 Participate in international watch, warning and incident response information sharing mechanisms.

2 - Actions:

IR 2.1 Identify or establish a national computer security incident response team (CSIRT) capability.
IR 2.2 Establish mechanism(s) for coordination within government among civilian agencies, law enforcement, the military and intelligence communities.
IR 2.3 Establish partnerships with the private sector for the prevention and response to cyber incidents.
IR 2.4 Establish point(s) of contact for consultation, cooperation, and information exchange among CSIRTs from government agencies, the military and intelligence communities, the private sector and international partners.
IR 2.5 Undertake international cooperative and information sharing activities.
IR 2.6 Develop tools and procedures for the protection of the cyber resources of government entities.

POLICY: *The protection of critical information infrastructure and cyberspace is a shared responsibility that requires a coordinated partnership between the government at all levels and the private sector, which owns and operates much of this information infrastructure.*

1 - Goals:

IG 1.1 Develop public-private partnerships for the protect cyberspace and globally interconnected information infrastructures.
IG 1.2 Develop cyber risk management program.

2 - Actions:

IG 2.1 Include industry perspectives in the development and implementation of security policy and efforts.
IG 2.2 Encourage development of industry and non-government (sector) groups to address security around common interests.
IG 2.3 Encourage cooperation among sector groups of interdependent industries.
IG 2.4 Establish cooperation arrangements between government and industry for watch, warning and incident response systems. (See also IR.)
IG 2.5 Support industry awareness raising efforts.
IG 2.6 Promote a comprehensive national awareness program to empower all participants – businesses, the general workforce, and the general population – to secure their own parts of cyberspace.
IG 2.7 Develop a framework for public-private partnership to address cyber risk based on threats, vulnerabilities and consequences.

POLICY: *Ever more powerful personal computers, converging technologies, the widespread use of the Internet; increasing interconnectivity and connections cross national borders require that all participants who develop, own, provide, manage, service and use information systems and networks be aware of and understand security issues and take action appropriate to their role to protect cybersecurity and cyber assets. Government must take a leadership role in bringing about this Culture of Security and supporting the efforts of other participants.*

1 - Goals:

CS 1.1 As part of national strategy, undertake efforts to promote a national Culture of Security consistent with UNGA Resolutions 57/239, *Creation of a global culture of cybersecurity*, and 58/199, *Creation of a global culture of cybersecurity and the protection of critical information infrastructures*.

2 - **Actions:**

CS 2.1 Implement security plan for government owned and operated systems and networks.
CS 2.2 Implement security awareness programs and initiatives for users of government systems and networks.
CS 2.3 Develop Culture of Security outreach partnerships with business and industry.
CS 2.4 Support outreach to civil society with special attention to the needs of children and individual users.
CS 2.5 Enhance S&T and R&D activities.