

Cyber Security and Critical Infrastructure Protection

Model National Plan

Page 2 of 2

National Strategy (NS)

Legal Foundation and Regulatory Development

Incident Response Watch, Warning, Recovery

Partnerships Industry - Government

Culture of Security

3 – Dialogue and Training Resources: (available from the U.S. or internationally)

NS 3.1 Awareness raising (Supports NS 2.1, 2.2)
OECD Guidelines and Culture of Security:
<http://webdomino1.oecd.org/COMNET/STI/ccpSecu.nsf?OpenDatabase>

- UNGA Resolutions 55/63, 56/121, 57/239, 58/199:
<http://www.un.org/Depts/dhl/resguide/gares1.htm>

NS 3.2 National Strategy (NS 2.2, 2.3, 2.4, 2.7)

- U.S. National Strategy to Secure Cyberspace:
<http://www.whitehouse.gov/pcipb/>

NS 3.3 Assessment and program development (NS 2.4, 2.5, 2.7, 2.8)

NS 3.4 International assistance points of contact (NS 2.6)

3 – Dialogue and Training Resources: (available from the U.S. or internationally)

LR 3.1 Executive Branch (LR 2.1, 2.6)

- Council of Europe: Convention on Cybercrime website:
<http://www.coe.int/T/E/Com/Files/Themes/Cybercrime/default.asp>
- UNGA Resolutions 55/63, 56/121:
<http://www.un.org/Depts/dhl/resguide/gares1.htm>
- G-8 High-Tech Crime Principles and 24X7 information assistance mechanism. (web site???)
- DOJ CCIPS website: <http://www.cybercrime.gov>
- APEC TEL Working Group E-Security Task Group Documents: <http://www.apectelwg.org/e-securityTG/index.htm>
- APEC TEL Cybercrime Legislation and Enforcement Capacity Building Project Resource Materials: <http://www.apectelwg.org/e-securityTG/Resources.htm>

LR 3.2 Legislative Branch (LR 2.2, 2.5)

- Council of Europe: Convention on Cybercrime website:
<http://www.coe.int/T/E/Com/Files/Themes/Cybercrime/default.asp>
- UNGA Resolutions 55/63, 56/121:
<http://www.un.org/Depts/dhl/resguide/gares1.htm>
- DOJ CCIPS website: <http://www.cybercrime.gov>
- APEC TEL Working Group E-Security Task Group Documents: <http://www.apectelwg.org/e-securityTG/index.htm>
- APEC TEL Cybercrime Legislation and Enforcement Capacity Building Project Resource Materials: <http://www.apectelwg.org/e-securityTG/Resources.htm>

LR 3.3 Judicial Branch (LR 2.2, 2.5)

- Council of Europe: Convention on Cybercrime website:
<http://www.coe.int/T/E/Com/Files/Themes/Cybercrime/default.asp>
- UNGA Resolutions 55/63, 56/121:
<http://www.un.org/Depts/dhl/resguide/gares1.htm>
- DOJ CCIPS website: <http://www.cybercrime.gov>
- APEC TEL Working Group E-Security Task Group Documents: <http://www.apectelwg.org/e-securityTG/index.htm>
- APEC TEL Cybercrime Legislation and Enforcement Capacity Building Project Resource Materials:
<http://www.apectelwg.org/e-securityTG/Resources.htm>

3 – Dialogue and Training Resources: (available from the U.S. or internationally)

IR 3.1 National Response Plan (IR 2.1-2.6)

- National Strategy:
http://www.dhs.gov/interweb/assetlibrary/NationalCyberspace_Strategy.pdf
- Industry: National Cyber Security Partnership:
<http://www.cyberpartnership.org/031804.html>
- StaySafeOnline
<http://www.staysafeonline.info/>
- Information Security and Privacy Advisory Board <http://csrc.nist.gov/ispab/>
- NIST: <http://csrc.nist.gov/>

IR 3.2 National CSIRT (IR 2.1-2.5)

- US CERT: <http://www.us-cert.gov/>
- Homeland Security Operations Center http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0456.xml
- NIATEC training courses: <http://niatec.info>

IR 3.3 Cooperation and Information Sharing (IR 2.1-2.5)

- Industry: National Cyber Security Partnership, Early Warning Task Force:
<http://www.cyberpartnership.org/031804.html>
- National Cyber Security Partnership, Public Awareness Task Force
<http://www.cyberpartnership.org/031804-3.html>
- IT-ISAC: <https://www.it-isac.org/>
- National Cyber Response Coordinating Group:
<http://www.dhs.gov/dhspublic/display?content=4359>
- <http://www.house.gov/science/hearings/full05/sep15/Purdy%20Testimony%20Final.pdf>
- Critical Infrastructure Protection Advisory Committee
http://www.itaa.org/infosec/docs/CIPAC_FactSheet2.pdf
- IT Sector Coordinating Council
<http://www.itaa.org/infosec/docs/ITSCCResponsesToGAO.pdf>

3 – Dialogue and Training Resources: (available from the U.S. or internationally)

IG 3.1 Structures for Industry-Government Partnership (IG 2.1, 2.2 and 2.7)

- ICSACS & Coordinating Councils
- ITAA White Paper on Information Security:
<http://www.itaa.org/infosec/doc/ITAAINIPPComments1.doc>
- ITAA Comments on DHS National Infrastructure Protection Plan:
<http://www.itaa.org/infosec/docs/ITAAINIPPComments1.doc>

IG 3.2 Cyber security and CIIP information sharing (IG 2.3, 2.4 and 2.7)

- National Information Assurance Council (NIAC) report on cross sector interdependencies:
[http://www.itaa.org/infosec/docs/Cross%20Sector%20Interdependencies%20WG%20Final%20Report_Redacted%20\(2003-10-06\).pdf](http://www.itaa.org/infosec/docs/Cross%20Sector%20Interdependencies%20WG%20Final%20Report_Redacted%20(2003-10-06).pdf)
- National Infrastructure Protection Plan (NIPP): <http://www.fbic.gov/reports/FR-NIPP.pdf>
- US-CERT alerts: <http://www.us-cert.gov/>
- National Cyber Alert System (NCAS):
<http://www.dhs.gov/dhspublic/display?content=3086>

IG 3.3 Awareness raising and outreach: Tools for business and home use (IG 2.5 and 2.6)

- Information for technical and non-technical users: <http://www.us-cert.gov/>
- StaySafeOnline:
<http://www.staysafeonline.org/>

3 – Dialogue and Training Resources: (available from the U.S. or internationally)

CS 3.1 Government systems and networks (CS 2.1, 2.2)

- The U.S. Federal Information Security Management Act of 2002 (FISMA)
<http://csrc.nist.gov/sec-cert/index.html>
- HSPD-7, "Critical Infrastructure Identification, Prioritization and Protection"
- Federal Acquisition Regulation (FAR), parts 1.2,7,11, and 39.
- The National Strategy to Secure Cyberspace:
http://www.dhs.gov/interweb/assetlibrary/nationalCyberspace_Strategy.pdf
- US CERT site: <http://www.us-cert.gov/>
- NIST site: <http://csrc.nist.gov/> and <http://csrc.nist.gov/fasp/> and <http://csrc.nist.gov/ispab/>

CS 3.2 Business and private sector organizations (CS 2.3, 2.5)

- National Cyber Security Partnership:
www.cyberpartnership.org
- US CERT: <http://www.us-cert.gov/>
- DHS/Industry "Cyber Storm" exercises:
<http://www.dhs.gov/dhspublic/display?content=5416>
- DHS R&D Plan:
http://www.dhs.gov/interweb/assetlibrary/ST_2004_NCIP_RD_PlanFINALApr05.pdf
- President's Information Technology Advisory Committee report on Cyber Security research priorities:
http://www.nitrd.gov/pitac/reports/20050301_cybsecurity/cybersecurity.pdf

CS 3.3 Individuals and civil society (CS 2.4)

- Stay Safe Online:
<http://www.staysafeonline.info/>
- US CERT: <http://www.us-cert.gov/nav/nt01/>
- See also: The USG response to the OECD questionnaire on implementation of a Culture of Security (DSTI/CCP/REG(2004)4/Final). Available together with responses from other OECD countries at the OECD security web site:
<http://webdomino1.oecd.org/COMNET/STI/ccpsecu.nsf?OpenDatabase>