

# Appendix 1B: International CI/KR Protection

## 1B.1 Introduction and Purpose of This Appendix

This appendix provides guidance for addressing the international aspects of CI/KR protection in support of the NIPP.

### 1B.1.1 Scope

The NIPP provides the mechanisms, processes, key initiatives, and milestones necessary to enable DHS, the Department of State, the SSAs, and other security partners to address international implications and requirements related to CI/KR protection. The NIPP and associated SSPs recognize that protective measures do not stop at a facility's fence line or a national border. Because disruptions in the global infrastructure can ripple and cascade around the world, the NIPP and SSPs also must consider cross-border CI/KR, international vulnerabilities, and global dependencies and interdependencies.

### 1B.1.2 Vision

The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets identifies “fostering international cooperation” as one of the eight guiding principles of its vision for the future. The strategy underscores the need for a coordinated, comprehensive, and aggressive global action as a key aspect of the NIPP approach to CI/KR protection.

Furthermore, the National Strategy to Secure Cyberspace sets forth strategic objectives for national security and international cyberspace security cooperation that deal directly with the international aspects of CI/KR protection, including preventing cyber attacks against America's critical infrastructure, reducing vulnerabilities, and minimizing damage and recovery time from cyber attacks and incidents that do occur.

### **1B.1.3 Implementing the Vision With a Strategy for Effective Cooperation**

The NIPP CI/KR international coordination and protection strategy outlined in this appendix is focused on instituting effective cooperation with international security partners, rather than on discussing specific protective measures. Specific protective measures are tailored to each sector's particular circumstance and are developed in the SSPs. This appendix also focuses on implementing existing agreements that affect CI/KR protection and addressing cross-sector and global issues such as cyber security.

The Department of State, DHS, and the SSAs will periodically review the international CI/KR protection strategy and redraft it, as needed, to ensure that it complements and supports specific objectives detailed in the NIPP.

Within 6 months of the approval of the NIPP, DHS, the Department of State, and other concerned Federal agencies will incorporate the NIPP into their strategies for cooperating with other countries and international/multinational organizations. This effort will focus on promoting a global culture of physical and cyber security, managing CI/KR-related risk as far as possible outside the physical borders of the United States; accelerating international cooperation to develop intellectual infrastructure based on shared assumptions and compatible conceptual tools; and connecting constituencies not traditionally engaged in security. The broad structure of this approach is outlined in this appendix; it is based on the following high-level considerations.

## **1B.2 Responsibilities for International Cooperation on CI/KR Protection**

In accordance with HSPD-7, the Department of State, in conjunction with DHS, DOJ, DOD, the Departments of Commerce and Treasury, the NRC, and other appropriate agencies, is responsible for working with foreign countries and international/multinational organizations to strengthen the protection of U.S. CI/KR. This section provides further details regarding the responsibilities of DHS and other security partners related to the international dimension of CI/KR protection.

### **1B.2.1 Department of Homeland Security**

Under the CI/KR risk management framework described in this plan, DHS, in collaboration with other security partners, is responsible for the following actions, all of which have an international dimension:

- Building security partnerships;
- Implementing a comprehensive, integrated risk management program; and
- Implementing protective programs.

DHS, in conjunction with the Department of State and in cooperation with other foreign affairs agencies, will share with international entities appropriate information and perform outreach functions to enhance information sharing and management of international agreements regarding CI/KR protection.

Some of the more complex challenges presented by the international aspects of CI/KR protection involve analyzing the complex dependencies, interdependencies, and vulnerabilities that require the application of sophisticated and innovative modeling techniques. DHS is responsible for pursuing research and analysis in this area. It will call on a range of outside sources for this work, including those with expertise in the international community and the NISAC.

### **1B.2.2 Department of State**

The Secretary of State has direct responsibility for policies and activities related to the protection of U.S. citizens and U.S. facilities abroad. The Secretary of State, in conjunction with the Secretary of Homeland Security, is responsible for coordinating with foreign countries and international organizations to strengthen the protection of U.S. CI/KR. The Department of State supports DHS and other Federal agency efforts by providing knowledge about and access to other governments. The Department of State

leverages bilateral and multilateral relationships around the world to ensure that the Federal Government can act effectively to identify and protect U.S. CI/KR.

The Department of State, DHS, and other agencies are engaged in a wide range of activities throughout the world to prevent, disrupt, and deter threats and acts of terrorism directed against the homeland and U.S. interests abroad. The objectives of these efforts are to develop and work with global partners to ensure mutual security and to raise awareness of the terrorist threat.

### **1B.2.3 Other Federal Agencies**

SSAs exchange information, including cyber-specific information, with security partners in other countries, in accordance with guidelines established by DHS and the Department of State and other agencies, as appropriate, to improve the Nation's overall CI/KR protection posture.

The Departments of Commerce and Treasury, DOJ, DOD, DOE, DOT, and other agencies share responsibility, in accordance with HSPD-7, for working through the Department of State to reach out to foreign countries and international organizations to strengthen the protection of U.S. CI/KR.

### **1B.2.4 State, Local, and Tribal Governments**

State, Territorial, local, and tribal governments ensure ongoing cooperation with relevant international, regional, local, and private sector CI/KR protection efforts.

### **1B.2.5 Private Sector**

DHS is working with the private sector, SSAs, private voluntary and nongovernmental organizations, and information-sharing mechanisms and organizations to protect cross-border infrastructure and understand international and global vulnerabilities. DHS relies on the private sector for data, expertise, and knowledge of their international operations to identify relevant international assets, systems, and networks, and assess risks and global vulnerabilities, including shared threats and interdependencies.

### **1B.2.6 Academia**

The academic community provides data, insight, and research into the significance of international interdependencies, modeling, and analysis.

## **1B.3 Managing the International Dimension of CI/KR Risk**

The NIPP addresses international CI/KR protection, including interdependencies and the vulnerability to threats that originate outside the country. The NIPP brings a new focus to international security cooperation and provides a risk-based strategic framework for measuring the effectiveness of international CI/KR protection activities. The NIPP also provides tools to assess international vulnerabilities and interdependencies that complement long-standing cooperative agreements with Canada, Mexico, the United Kingdom, NATO, and others, and provides a framework for effective collaborative engagement with additional international partners.

SSPs are required to include international considerations as an integral part of each sector's planning process rather than instituting a separate layer of planning. Some international aspects of CI/KR protection require additional overarching or cross-sector emphasis. These include:

- U.S. interaction with foreign governments and international organizations to enhance the confidentiality, integrity, and availability of cyber-based infrastructure that often has an international or even global dimension;

- Protection of physical assets located on, near, or extending across the borders with Canada and Mexico that require cooperation with and/or planning and resource allocation among neighboring countries, States bordering on these countries, and affected local and tribal governments;
- Sectors with CI/KR that are extensively integrated into an international or global market (e.g., Banking and Finance or other information-based sector, Energy, or Transportation) or when the proper functioning of a sector relies on inputs that are not within the control of U.S. entities; and
- U.S. Government and corporate facilities located overseas that may be regarded as CI/KR may be determined to be critical based on implementation of the NIPP framework. Protection for the Government Facilities sector involves careful inter-agency collaboration, as well as cooperation with foreign CI/KR security partners.

The following subsections discuss issues associated with the international aspects of CI/KR protection in the context of the steps of the NIPP risk management process. (See NIPP Chapter 3, The Protection Program Strategy: Managing Risk.)

### 1B.3.1 Setting Security Goals

The overarching goal of the NIPP—to enhance the protection of U.S. CI/KR—applies to the international “system of systems” that underpins U.S. CI/KR. The NIPP and the SSPs provide guidance and risk management approaches that address the international aspects of CI/KR protection efforts on both a national and a sector-specific basis. In addition, a separate set of goals and priorities guide cross-sector efforts to improve protection for CI/KR with international linkages. These goals fall into three categories:

- Identifying and addressing cross-sector and global issues;
- Implementing existing and developing new agreements that affect CI/KR; and
- Improving the effectiveness of international cooperation.

DHS, in conjunction with the Department of State and other security partners, will define the requirement for a comprehensive international CI/KR protection strategy. The integration of international CI/KR protection considerations and measures into the SSPs is important for pursuing and achieving these goals in ways that complement each other and are achievable with the resources available.

Important considerations in achieving these goals are discussed in this section; actions required to achieve these goals are addressed in the section on key implementation actions.

### 1B.3.2 Identifying CI/KR Affected by International Linkages

Once international security goals are set, the next step in the risk management process is to develop and maintain a comprehensive inventory of the Nation’s CI/KR outside U.S. borders and of foreign CI/KR that may affect systems within this country. The process for identifying nationally critical CI/KR involves working with U.S. industry, SSAs, academia, and international partners to gather and protect information on the foreign infrastructure and resources on which U.S. CI/KR rely.

**Dependency and Interdependency and International CI/KR Protection Cooperation:** The NIPP risk management framework details a structured approach for use in determining dependencies and interdependencies, including physical, cyber, and international considerations. This approach is designed to address CI/KR protection in three areas:

- Direct international linkages to physical and cyber U.S. CI/KR:
  - Foreign cross-border assets linked to U.S. CI/KR, such as roads, bridges, pipelines, gas lines, telecommunications lines and undersea cables and facilities, and power lines, etc., physically connecting U.S. CI/KR to Canada and Mexico;

- Foreign infrastructure whose disruption or destruction could directly harm the U.S. homeland, such as waters behind a Canadian dam that could flood U.S. territory or a toxic plume from an impacted Mexican chemical plant that could contaminate U.S. territory, or foreign ports where security failures could directly affect U.S. security; and
- U.S. CI/KR that may be located overseas, such as non-military government facilities, are overseas components of U.S. CI/KR;
- Indirect international linkages to physical and cyber U.S. CI/KR:
  - The potential cascading and escalating effects of disruption or destruction of foreign assets, systems, and networks; critical foreign technology; goods; resources; transit routes; and chokepoints; and
  - Foreign ownership, control, or involvement in U.S. CI/KR and related issues; and
- Global aspects of physical and cyber U.S. CI/KR:
  - Assets, systems, and networks either located around the world or with global mobility that require the efforts of multiple foreign countries to secure.

Dependency and interdependency analysis is primarily based on information from each sector and is formulated by the judgments of CI/KR owners and operators regarding their supply chains and sources of services from other infrastructure sectors, such as Energy and Water. As the capability for sophisticated network analysis grows, these inputs will be complemented by assessments that examine less apparent network-based dependencies and interdependencies. The NISAC supports this effort by analyzing and quantifying national and international dependency and interdependency for complex systems and networks that affect specific sectors.

### 1B.3.3 Assessing Risks

The risk assessment for CI/KR assets, systems, and networks that are affected by international linkages is an integral part of the risk management framework described in the NIPP. The risk management framework combines consequences, threats, and vulnerabilities to produce systematic and comprehensive risk assessments that can be clearly explained in a three-step process:

- Determining the consequences of destruction, incapacitation, or exploitation of an asset, system, or network. This is done to assess potential national significance, as well as physical, cyber, and human dependencies and interdependencies that may result from international linkages.
- Analyzing vulnerability, including determining which elements of CI/KR are most susceptible to attack or other disruption, and whether attacks against these elements could be a consequence of any international linkages.
- Conducting a threat analysis that provides the likelihood that a target will be attacked. CI/KR with international linkages may present greater opportunities for attack and thus increase the likelihood that they may be the subject of attacks.

Issues important to the other countries may be different from those for the United States. Risk analysis needs to be conducted in coordination with other countries in order to draw on their analysis, as well as our own.

### 1B.3.4 Prioritizing

Assessing CI/KR on a level playing field that adjudicates risk based on a common framework ensures that resources are applied where they offer the most benefit for reducing risk; deterring threats; and minimizing the consequences of attacks, natural disasters, and other emergencies. The same prioritization used for domestic CI/KR protection is observed to evaluate the risk arising from international linkages. The priority for protection investments could be raised if international linkages increase the risk.

### 1B.3.5 Implementing Programs

The SSAs have primary responsibility for developing protective measures that address risks that arise from international factors. In addition to sector protective measures, DHS has specific programs to help enhance the cooperation and coordination needed to address the unique challenges posed by the international aspects of CI/KR protection:

- **International Outreach Program:** DHS works in conjunction with the Department of State and with other foreign affairs agencies to conduct international outreach with foreign countries and international organizations to encourage the promotion and adoption of organizational and policymaking structures, information-sharing mechanisms, industry partnerships, best practices, training, and other programs as needed to improve the protection of overseas assets and the reliability of foreign infrastructure on which the United States depends.
- **The National Cyber Response Coordination Group:** The NCRCG facilitates coordination of the Federal Government's efforts to prepare for, respond to, and recover from cyber incidents and physical attacks that have significant cyber consequences (collectively known as cyber incidents). It serves as the Federal Government's principal interagency mechanism for operational information sharing and coordination of Federal Government response and recovery efforts during a cyber incident. The NCRCG considers and consults with international partners on a regular basis for routine situational awareness and during incidents. NCRCG member agencies integrate their capabilities to facilitate assessment of the domestic and international scope and severity of a cyber incident.
- **The National Exercise Program:** DHS provides overarching coordination for the National Exercise Program to ensure the Nation's readiness to respond in an all-hazards environment and to test the steady-state protection plans and programs put in place by the NIPP. The exercise program, as appropriate, engages international partners to address cooperation and cross-border issues, including those related to CI/KR protection. DHS and other security partners also participate in exercises sponsored by international partners, including cross-border, multi-sector tabletops.
- **National Cyber Exercises:** DHS is conducting exercises to identify, test, and improve coordination of the cyber incident response community, including Federal, State, Territorial, local, tribal, and international government elements, as well as private sector corporations and coordinating councils.

Because of the complex nature of the international dimension of CI/KR, a substantial emphasis is placed on best practices that can be used to improve cooperation and coordination. To this end, DHS will lead efforts to:

- Collaborate to establish global best practices, successful protection measures, and best practices related to telecommunications, air transportation systems, container shipping, cyber security, and other global systems as appropriate;
- Encourage the development and adoption of, and adherence to, standards of the International Organization for Standards and similar organizations that can help to reduce insurance premiums and level CI/KR protection costs for businesses; and
- Work with international security partners to determine the appropriate threshold for engagement with countries on cyber issues.

### 1B.3.6 Measuring Effectiveness and Making Improvements

The NIPP specifies three types of quantitative indicators to measure program effectiveness:

- **Descriptive Metrics** are necessary to understand sector resources and activities; they do not reflect CI/KR protection performance;
- **Process Metrics** measure whether specific activities were performed as planned; these track the progression of a task or report on the completion of an enabling process, such as forming a bilateral partnership; and
- **Outcome Metrics** track progress toward a strategic goal by beneficial results rather than level of activity.

The NIPP also distinguishes between two groups of metrics: core metrics that enable comparison and analysis between and among different sectors and sector-specific metrics that are useful within a sector.

Because protective measures are designed, implemented, and evaluated through sector-specific mechanisms guided by the SSPs, they deal with the protection challenges for a particular facility, network, or sector rather than international issues that may affect protection measures. Conversely, most initiatives that address the international issues affecting CI/KR protection are enablers rather than protective measures themselves. As a result, the metrics used to measure the effectiveness of international CI/KR protection initiatives will primarily be process metrics in the core group of CI/KR protection metrics. These will measure progress on tasks that enable CI/KR protection in situations that have international ramifications.

These metrics will be used to manage the comprehensive international CI/KR protection strategy, which enables SSP protection initiatives, and to track progress toward the strategy's three goals:

- Improving the effectiveness of international cooperation;
- Implementing existing and developing new agreements that affect CI/KR; and
- Addressing cross-sector and global CI/KR protection issues.

DHS, in cooperation with other Federal agencies, will develop the metrics to track progress on international CI/KR protection enablers. Examples of such metrics include:

- The international issues being faced by each sector, which of these affect multiple sectors, and which issues are the most important;
- The countries that should be involved in protection partnerships for each sector;
- The number and type of bilateral and multinational agreements affecting CI/KR protection;
- The nature, level of implementation, and effectiveness of bilateral and multinational agreements;
- The sectors affected by each international partnership;
- The number and type of outcomes enabled by an international initiative; and
- Where possible, the specific CI/KR protection enhancements that are directly attributable to a particular international initiative.

Once the core metrics have been developed and approved, DHS, the SSAs, and other security partners will collaborate to establish a data-gathering and reporting process. This process will outline, but will not be limited to, responsibilities; data collection, reporting procedures, and timeframes; metrics calculation; and the schedule for computing and updating the metrics on a regular basis.

## **1B.4 Organizing International CI/KR Protection Cooperation**

DHS, in conjunction with the Department of State and other Federal agencies, works with individual foreign governments, and regional and international organizations in partnership to enhance the protection of the Nation's CI/KR and to deny the exploitation of CI/KR assets. Potential partnerships depend on:

- Physical proximity to the United States or U.S. assets;
- Useful experience and information to be gained from other countries;
- Existing alliances, agreements, and high-level commitments;

- Critical supply chains and vulnerable nodes; and
- Interdependencies and networked technologies, and the need for a global “culture of security” to protect physical, cyber, and human assets.

As international CI/KR protection partnerships mature, cooperative efforts will strengthen in two dimensions:

- Development of new partnerships with countries possessing useful experience and information regarding CI/KR protective efforts, as well as terrorism prevention, preparedness, response, and recovery; and
- Development of new international relationships and institutions to protect global infrastructure and address international interdependencies, networked technologies, and the need for a global culture of physical and cyber security.

The coordination mechanisms supporting the NIPP create linkages between CI/KR protection efforts at the national, sector, State, regional, local, tribal, and international levels. The entities and bodies that are involved with this coordination are diverse and depend on the specifics of the issues they address, as well as other considerations as discussed in the following subsections.

#### **1B.4.1 Domestic Aspects of International CI/KR Protection Cooperation**

**Interagency Coordination—Department of State and DHS Leadership:** DHS will work with the Department of State, international partners, and with U.S. entities involved with the international aspects of CI/KR protection to exchange experiences, share information, and develop a cooperative atmosphere to materially improve U.S. CI/KR protection, information sharing, cyber security, and global telecommunications standards. DHS and SSAs will work with specific countries to identify international interdependencies and vulnerabilities. SSAs will consider such international factors as cross-border infrastructure, international vulnerabilities, and global interdependencies in their SSPs.

**Interagency Coordination—Review of Existing Mechanisms to Support the NIPP:** The International Affairs offices in Federal Government agencies maintain existing relationships with foreign counterpart ministries and agencies, and are the primary partners with the Department of State in coordinating with foreign governments on international CI/KR matters.

DHS also works with SSAs to ensure that SSPs reflect international factors, such as cross-border infrastructure, international interdependencies, and global vulnerabilities.

The Department of State presently chairs an interagency working group that coordinates U.S. international CI/KR protection outreach activities. Within 30 days of publication of this plan, the Department of State and DHS will review the working group’s charter and its coordination mechanisms to ensure that they address all international CI/KR issues specified by the NIPP. The Department of State and DHS, in coordination with other interagency working group members, will, within an additional 30 days, implement any changes needed to ensure that all NIPP requirements will be met and that the working group’s charter reflects a role that best supports the comprehensive international CI/KR protection strategy.

#### **1B.4.2 Foreign Aspects of International CI/KR Protection**

International cooperation on cyber security and other CI/KR protection issues (e.g., energy supplies) of a global nature is necessary because of the cross-border or borderless nature of these infrastructures. These efforts require interaction on both the policy and the operational levels and involve a broad range of entities from both the government and the private sector. Interaction on the international aspects of CI/KR protection takes place bilaterally, regionally, and multilaterally:

- **Bilateral:** DHS, in conjunction and consultation with the Department of State, participates in bilateral discussions and programs with countries of interest where issues are best addressed on a country-to-country basis.
- **Regional:** DHS and the Department of State partner together to provide leadership in regional groups, such as the OAS and the Asia-Pacific Economic Cooperation, to raise awareness and develop cooperative programs.

The United States engages with Canada and Mexico, as regional neighbors, on CI/KR protection to enhance collaboration efforts. Current activities include the United States, Canada, and Mexico trilateral SPP; the U.S.-Canada Critical Infrastructure Protection Framework for Cooperation (Smart Border Action Plan); and the U.S.-Mexico Critical Infrastructure Protection Framework for Cooperation (Border Partnership Action Plan).

- **Multilateral:** Multilateral collaboration on this aspect of CI/KR involves initiatives on the part of the OECD, G8, and United Nations. For the cyber security aspects of global CI/KR protection, DHS has established a preliminary framework for cooperation on cyber security policy, watch and warning, and incident response for CI/KR with key allies such as Australia, Canada, New Zealand, and the United Kingdom. DHS is coordinating and participating in the establishment of an IWWN among cyber security policy, computer emergency response, and law enforcement participants of 15 countries. The IWWN will provide a mechanism for the participating countries to share information to build cyber situational awareness and coordinate incident response.

### 1B.4.3 Working With Specific Countries and International Organizations

DHS, SSAs, and other security partners will work with other countries to promote CI/KR protection best practices and they will pursue infrastructure security through international/multinational organizations such as the G8, NATO, European Union, OAS, OECD, and Asia-Pacific Economic Cooperation. The approach to working with some specific countries and organizations is founded on formal agreements that address cooperation on CI/KR protection.

- **Canada and Mexico:** The CI/KR relationships between the United States and its immediate neighbors make the borders virtually transparent. Electricity, natural gas, oil, telecommunications, roads, rail, food, water, minerals, and finished products cross the borders on a regular basis as part of normal commerce. The importance of this trade, and the infrastructure that supports it, was highlighted after the terrorist attacks of September 11, 2001, nearly closed both borders. The United States entered into the 2001 Smart Border Declaration with Canada and the 2002 Border Partnership Declaration with Mexico, in part, to address bilateral CI/KR issues. In addition, the 2005 SPP established a trilateral approach to common security issues. The SPP is based on the principle that the prosperity of all three nations is dependent on mutual security. The SPP complements, rather than replaces, existing agreements.
- **United Kingdom:** The United Kingdom is a close ally with much experience in fighting terrorism and protecting its CI/KR. The United Kingdom has developed substantial expertise in law enforcement and intelligence systems, and in the protection of commercial facilities based on its experience in countering terrorism. Like the United States, most of the critical infrastructure in the United Kingdom is under private management. The government of the United Kingdom has developed an effective, sophisticated system of managing public-private partnerships. DHS has formed a JCG with the United Kingdom that brings officials into regular, formal contact to discuss and resolve a range of bilateral homeland security issues.
- **G8:** In the recent terrorist attacks against the United States, Spain, and the United Kingdom, the infrastructure in G8 countries was exploited and used to inflict casualties and fear. The G8 has underscored its determination to combat all forms of terrorism and to strengthen international cooperation. Counterterrorism work has been the focus of a number of initiatives launched at recent summits. At their meeting in Gleneagles Hotel in Scotland, in July 2005, the G8 heads of government issued a Statement on Counter-Terrorism. In it, they pledged to “commit ourselves to new joint efforts. We will work to improve the sharing of information on the movement of terrorists across international borders, to assess and address the threat to the transportation infrastructure, and to promote best practices for rail and metro security.” DHS will work closely with the G8 to address the common threats to CI/KR and cyberspace.
- **European Union:** The European Union is pursuing CI/KR as a matter of policy, noting that an effective strategy should focus on both preparedness and on consequence management. DHS will engage the European Union early in this process to share its experience, and to further cooperate on characteristics and common vulnerabilities of critical infrastructure and cyberspace, risk analysis techniques, and strategies to mitigate risk and minimize consequences.

- **North Atlantic Treaty Organization:** NATO addresses CI/KR issues through the Senior Civil Emergency Planning Committee, the senior policy and advisory body to the North Atlantic Council on civil emergency planning and disaster relief matters. The committee is responsible for policy direction and coordination of Planning Boards and Committees in the NATO environment. It has developed considerable expertise that applies to CI/KR protection and has planning boards and committees covering ocean shipping, inland surface transport, civil aviation, food and agriculture, industrial preparedness, civil communications planning, civil protection, and civil-military medical issues. DHS has a delegation to the Senior Civil Emergency Planning Committee at NATO, participates in NATO's telecommunications working group, and engages with NATO in preparedness exercises.

#### **1B.4.4 Foreign Investment in U.S. CI/KR**

CI/KR protection may be affected by foreign investment and ownership of sector assets. At the Federal level, this issue is monitored by the CFIUS. The committee is chaired by the Secretary of the Treasury, with membership including the Secretaries of State, Defense, Commerce, and Homeland Security; the Attorney General; the Directors of the OMB and the OSTP; the U.S. Trade Representative; the Chairman of the Council of Economic Advisers; the Assistant to the President for Economic Policy; and the Assistant to the President for National Security Affairs.

DHS has important responsibilities regarding various government commissions that support the NIPP. These include:

- As a member of the CFIUS, DHS examines the impact of proposed foreign investments on CI/KR protection. The committee coordinates the development and negotiation of security agreements with foreign entities that may be necessary to manage the risk to CI/KR that a foreign investment may pose. DHS leads government monitoring activities aimed at ensuring compliance with these agreements.
- DHS acts as a partner with DOJ and other executive branch departments in supporting executive branch reviews of applications to the FCC from foreign entities pursuant to section 214 of the Communications Act of 1934 to assess if they pose any threat to CI/KR protection.

#### **1B.4.5 Information Sharing**

Effective international cooperation of CI/KR protection requires a system for information sharing that includes processes and protocols for updates among all partners, mechanisms for systematic sharing of best practices, and frequent opportunities for partners to meet to discuss and address international CI/KR issues.

The NOC serves as the Nation's hub for information sharing and situational awareness for domestic incident management and is responsible for increasing coordination (through the NICC) among those members of the international community who are involved because of the role they play in enabling the protection of U.S. CI/KR.

The HSIN supports ongoing information-sharing efforts by offering COIs for selected international partners requiring close coordination with the NOC.

DHS also provides mechanisms, such as the US-CERT portal, to improve information sharing and coordination among government communities and selected international security partners for cyber security. Additionally, the Cybercop portal is a secure Internet-based information-sharing mechanism for law enforcement members involved in the field of electronic crimes investigation. This secure, Internet-based collaborative tool links and supports the law enforcement and investigative community worldwide, serving participants from more than 40 countries.

## 1B.5 Integration With Other Plans

The NIPP brings a new focus to international security cooperation and provides a risk-based strategic framework for measuring the effectiveness of international activities. The NIPP processes serve as management tools to assess international vulnerabilities and interdependencies. The NIPP process complements long-standing cooperative agreements with Canada, Mexico, the United Kingdom, NATO, and others, and provides the framework for collaborative engagement with additional international partners.

SSPs will include descriptions of sector relationships and security partner roles and responsibilities that address international/multinational organizations and foreign governments. SSPs also will provide a comprehensive view of CI/KR, including the dependencies and interdependencies; international links; and cyber systems needed for the sector to function.

## 1B.6 Ensuring International Cooperation Over the Long Term

The effort to ensure a sustainable approach to addressing the international aspects of CI/KR protection over the long term requires special consideration in the following areas:

- **Awareness:** Awareness of international aspects of CI/KR protection issues helps ensure implementation of effective, coordinated, and integrated CI/KR protection measures and enables CI/KR security partners to make informed decisions. Often these issues are not apparent to those who can take the most effective action because of the complexity of the international systems affecting CI/KR protection. Awareness programs designed to identify such issues and provide the common framework that allows these issues to be effectively addressed by security partners are required for continued support for protection programs over the long term.
- **Training and Education:** NIPP training topics for the managers and staff responsible for CI/KR that require emphasis include international considerations for CI/KR protection because of the complex considerations that often accompany international linkages and initiatives. Because training and education programs can result in a higher quality workforce for international security partners, they provide benefits over entire careers rather than on a one-time basis as direct aid to international partners often does. Additionally, DHS will ensure that the organizational and sector expertise needed to implement the international aspects of the NIPP program over the long term is developed and maintained through exercises that include adequate testing of international CI/KR protection measures and plans.
- **Research and Development:** Cooperative and coordinated research efforts are one of the most effective ways to improve protective capabilities or to dramatically lower the costs of existing capabilities so that international security partners can afford to do more with their limited budgets. Techniques and designs developed through research can cost very little to share with international security partners and, although the lead times needed for maturation of technology from the laboratory to the field can be decades, such improvements can have wider applicability or much greater effectiveness than available through current methods.
- **Plan Update:** NIPP and SSP updates must reflect the current international situation and must be coordinated, as required, with international agreements affecting CI/KR protection.