National Infrastructure Protection Plan

Information Sharing

The National Infrastructure Protection Plan (NIPP) sets forth a comprehensive risk management framework and clearly defines critical infrastructure protection roles and responsibilities for Federal, State, local, tribal, territorial, and private sector partners. The NIPP provides a coordinated approach that is used to establish national priorities, goals, and requirements for infrastructure protection so that funding and resources are applied in the most effective manner.

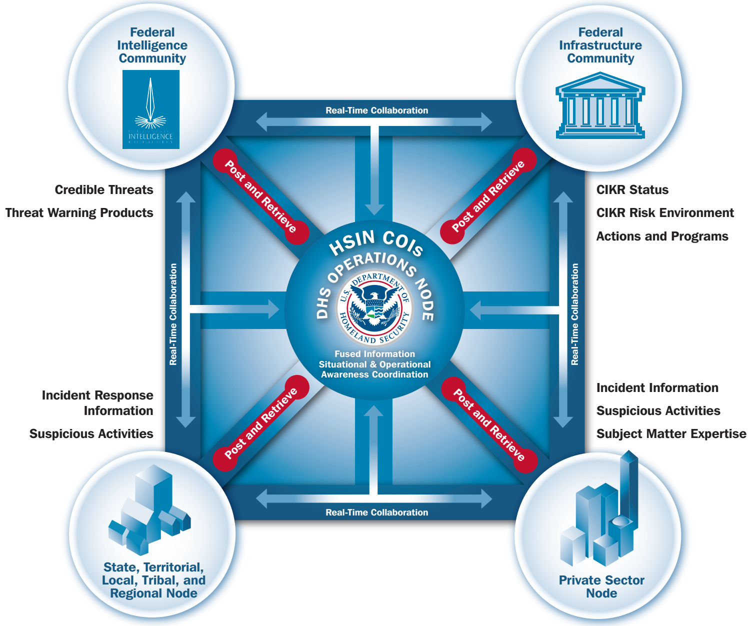
The NIPP is based on strong public-private partnerships that foster relationships and facilitate coordination within and across the Nation's critical infrastructure and key resources (CIKR) sectors. Consequently, the effective implementation of the NIPP depends on the degree to which government and private sector partners engage in effective, multi-directional information sharing. When owners and operators receive a comprehensive picture of threats or hazards to CIKR and participate in ongoing information flow, their ability to assess risks, make security investments, and take protective actions is substantially enhanced. Similarly, when the government is equipped with an understanding of private sector information needs, it can adjust its information collection, analysis, synthesis, and dissemination activities accordingly.

Establishing an information-sharing network that facilitates the protection of CIKR is a priority for Federal, State, local, tribal, territorial, and private sector partners. The ultimate goal is to create a nationwide network in which all CIKR partners may effectively collaborate to prepare for, protect against, respond to, and recover from a terrorist attack, national disaster, or other emergency. To enable the protection of CIKR, the Department of Homeland Security established an information-sharing network that is guided primarily by the NIPP and works in coordination with the efforts of the Federal Information Sharing Environment (ISE).

The ISE is concerned with improving the overall effectiveness of information sharing between and among Federal, State, and local government and the private sector. It is an element of the Intelligence Reform and Terrorism Prevention Act of 2004. The *Implementation Plan* for the ISE, published in December 2006, seeks to establish:

> A trusted partnership among all levels of government in the United States, the private sector, and our foreign partners, in order to detect, prevent, disrupt, preempt, and mitigate the effects of terrorism against the territory, people, and interests of the United States by the effective and efficient sharing of terrorism and homeland security information.

In April 2007, the National ISE Program Manager announced the adoption of the CIKR ISE, developed under the NIPP, as the private sector component of the Federal ISE. The ISE



Program Manager also designated the DHS Assistant Secretary for Infrastructure Protection as the Executive Agent for integrating the private sector and the information-sharing network developed under the NIPP into the Federal ISE.

The sector partnership model is the key public-private sector coordination structure under the NIPP. It includes CIKR owners and operators, their trade association representatives, and government agencies and officials carrying out responsibilities relevant to their CIKR protection missions. There are five key components to the CIKR ISE. They are: coordination and governance; risk mitigation; relationship management; information exchange; and content identification and development. Within the CIKR ISE, owners and operators can exchange comprehensive risk, threat, and hazard information to enhance their ability to assess risks to CIKR assets, make prudent security investments, and take more appropriate and meaningful protective actions, including incident response and recovery.

The CIKR ISE is currently being implemented through the systemic development of information-sharing policies and the coordinated public-private sector implementation of core and enhanced mission-related information-sharing processes. For each level of decision-making and action, the CIKR ISE fosters the development of policy and governance processes. This ensures coordination, clear identification of roles and responsibilities, and the technological and content requirements needed to make information exchange effective and valued. Over the last year, DHS has assisted each sector with identifying or developing an effective and efficient information-sharing environment suited to their unique characteristics. The process that has emerged for this systematic development reflects a maturing process that each sector undergoes within the CIKR ISE Capability Maturity Model (CMM). The capabilities that each sector develops in this model include:

- Information-Sharing Governance;
- Membership;
- Alerts, Warnings and Notifications (AWN);
- Suspicious Activity Reporting (SAR);
- Document Management;
- Incident Collaboration and Coordination (IC&C); and
- Routine Collaboration and Coordination (RC&C).

The CIKR ISE continues to mature and make substantial progress. For example, the National Infrastructure Coordination Center (NICC) is recognized as the hub for 24x7 operations by the sectors, particularly during incident response and recovery. The Homeland Security Information Network acquired substantial enhanced functionality and Protective Security Advisors (PSAs) have significantly expanded their capabilities to develop and manage relationships with individual owners and operators of CIKR "on the ground." Many State and local government representatives have stated that PSAs are invaluable sources of information on national policy, programs, and activities.

The NIPP provides the singular focus and unifying framework to advance the Department's mission to protect and secure the Nation by protecting CIKR. This mission focuses and drives implementation of the CIKR ISE to ensure its usefulness to all partners.

Homeland Security

For questions or more information, please contact NIPP@dhs.gov or visit www.dhs.gov/nipp.