National Infrastructure Protection Plan

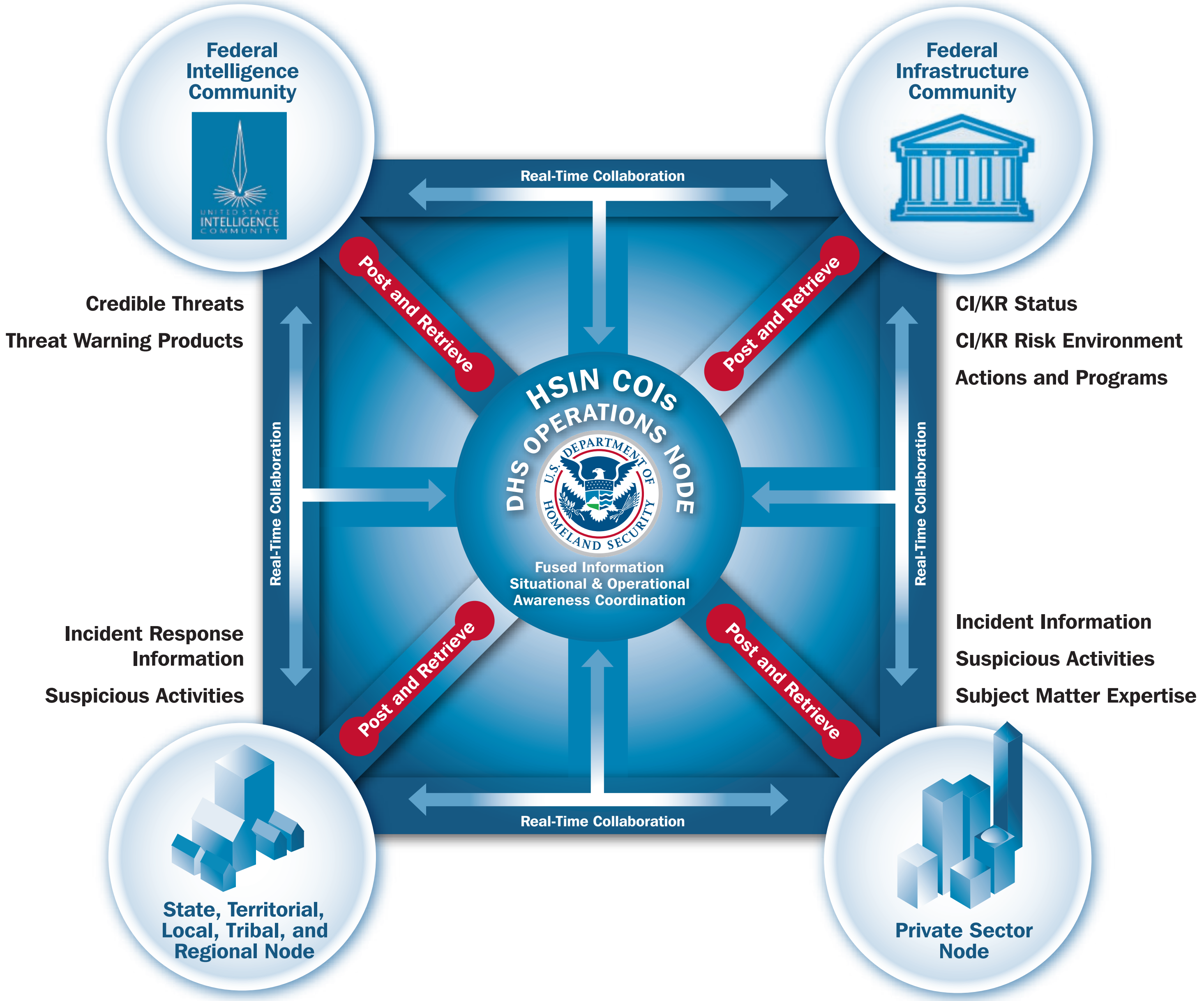
Information Sharing

The National Infrastructure Protection Plan (NIPP) sets forth a comprehensive risk management framework and clearly defines critical infrastructure protection roles and responsibilities for the Department of Homeland Security, Federal Sector-Specific Agencies, and other Federal, State, local, tribal, and private sector security partners. The NIPP provides the coordinated approach that will be used to establish national priorities, goals, and requirements for infrastructure protection so that funding and resources are applied in the most effective manner.

The effective implementation of the NIPP is predicated on active participation by government and private sector security partners in robust multi-directional information sharing. When owners and operators are provided with a comprehensive picture of threats or hazards to critical infrastructure and key resources (CI/KR) and participate in ongoing multi-directional information flow, their ability to assess risks, make prudent 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.

The NIPP information-sharing approach constitutes a shift from a strictly hierarchical to a networked model, allowing distribution and access to information both vertically and horizontally, as well as the ability to enable decentralized decision making and actions. The objectives of the networked approach are to:

- Enable secure multi-directional information sharing between and across government and industry that focuses, streamlines, and reduces redundant reporting to the greatest extent possible;
- Implement a common set of communications, coordination, and information-sharing capabilities for all security partners;
- Provide security partners with a robust communications framework tailored to their specific information-sharing requirements, risk landscape, and protective architecture;
- Provide security partners with a comprehensive common operating picture that includes timely and accurate information about natural hazards, general and specific terrorist threats, incidents and events, impact assessments, and best practices;



- Provide security partners with timely incident reporting and verification of related facts that CI/KR owners and operators can use with confidence when considering how evolving incidents might affect their security posture;
- Provide a means for State, local, tribal, and private sector security partners to be integrated, as appropriate, into the intelligence cycle, to include providing inputs to the intelligence requirements development process;
- Enable the flow of information required for security partners to assess risks, conduct risk management activities, invest in security measures, and allocate resources; and
- Protect the integrity and confidentiality of sensitive information.

The information-sharing process is designed to communicate both actionable information on threats and incidents and information pertaining to overall CI/KR status (e.g., plausible threats, vulnerabilities, potential consequences, incident situation, and recovery progress) so that owners and operators, States, localities, tribal governments, and other security partners can assess risks, make appropriate security investments, and take effective and efficient protective actions.

Homeland Security

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