



Governing Principles for Information Sharing

The Need to Share Information

1. The appropriate sharing of information between and among CI/KR sectors and governments will help protect and recover critical infrastructures.
 - Dissemination of critical infrastructure information must be made to the appropriate organizations and individuals in both private sector and government organizations; and both the government and private sector will work to ensure that mechanisms will be established with the greatest efficiency and necessary security possible.
 - Mechanisms are needed to vet those who participate in an information-sharing network to safeguard sensitive and proprietary information.
 - Sector expertise can determine the relevance of information and provide context to the data when it is shared with other sectors or government.
 - Sectors should determine appropriate dissemination mechanisms and recipients of information, considering any or all of: DHS, SSAs, ISAC, HSIN, US-CERT, and other sectors.
 - Sharing situational awareness information during incidents is important to all sectors to ensure coordinated response and minimize interdependency vulnerabilities.
2. Information sharing is vital to effective prevention, response, and recovery activities.
 - Private-sector organizations (PCIS, Sector Coordinating Councils, ISAC Council, ISACs, etc.) should regularly review after-action reports from incidents and exercises for lessons learned related to information sharing and successful protective measures.
3. The type of information shared and the methods and protocols for sharing information may vary among the CI/KR sectors.
 - Information needed by and provided to individual sectors will vary and need to reflect the unique characteristics of each sector; one size does not fit all.
 - Sharing information across sectors and with government will present challenges to ensure the information is timely and meaningful.

Managing the Risks Associated with Sharing Information

4. A risk-informed approach will be used to ensure that information related to threats and vulnerabilities will be shared when the benefits outweigh the risks associated with sharing the information.
 - The decision to share information needs to be timely and executed swiftly.



Governing Principles for Information Sharing

- Assigning private-sector individuals to coordinate with the Federal government (including HITRAC and other members of the intelligence community) fosters improved understanding of “need to know” and builds collaboration and trust.
 - Subject-matter experts from the private sector can determine the relevance of information for each sector.
 - Government- and industry-specific intelligence information drives appropriate alert levels and responses.
5. Information sharing must not violate applicable laws, regulations, or statutes and must incorporate protection mechanisms for proprietary information.

Managing the Information Sharing Process

6. The originator of information to be shared is considered to be the owner of that information, and is accountable for deciding if and how information will be shared.
- The concept of “originator control” needs to be recognized and respected as an essential element of successful information sharing.
 - Originators must understand how their information will be disclosed and/or used.
7. Policies, operational procedures, and protocols are needed to disseminate, control, and limit disclosure to protect shared information.
- Trusted information sharing between and among sectors is vital. Private-sector companies must know that their information is protected from inadvertent disclosure to those whose actions may result in unintended disadvantage to the originator, including competitors and regulatory agencies.
 - The private sector encourages improvements to the Protected Critical Infrastructure Information (PCII) Program and the development of operational procedures that will enhance the private sector’s ability to share information appropriately.