

POSITION STATEMENT

Critical Infrastructure Protection

*Adopted by the IEEE-USA
Board of Directors (26 June 2009)*

Critical infrastructures are those systems and assets -- both physical and cyber -- so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, economic security, the environment, public health, and safety. IEEE-USA is committed to making recommendations that will support and enhance not only the safety, but also the economic growth of the nation.

IEEE-USA recommends that the measures for critical infrastructure protection being developed by the Congress, Federal Agencies, State Legislatures and Agencies, and the private sector focus on the following:

1. Safeguard information technology used to manage critical infrastructures in order to mitigate the consequences of intentional or unintentional disruptions.

- Provide for resilient system failure architecture including progressive restoration of services
- Ensure adequate hardware components are immediately available for progressive restoration of services; widespread disruptions/disasters may cause delays in hardware acquisition
- Provide redundant backup of data, in a geographically diverse location, to facilitate disaster recovery
- Control access to selected devices, information, or both, to protect against unauthorized access of the device or information
- Restrict the flow of data to unauthorized recipients and functions
- Work to ensure consistent transparency, education and accountability across organizational boundaries including government and non-government entities
- Support research, development and education to strengthen information security across government and non-government entities.

2. Provide technology, policy and educational support to detect threats and monitor for potential hazards, and disseminate this information in synthesized form.

- Support open education and training in technology and processes to government, individuals and non-government entities
- Ensure the integrity of data on selected communication channels to protect against unauthorized changes

- Ensure the confidentiality of data on selected communication channels to protect against eavesdropping
- Support research and development on networks to monitor and disseminate warnings of hazards, cyber security threats, and invasion of privacy and
- Support research and development to predict or simulate effects of possible hazards, such as blackouts, Katrina, other disasters -- events that have a huge impact on critical infrastructure. Ensure this information is disseminated outside the government to non-government entities, including private and commercial. Plan, train, and assist Community and Individual Resiliency and Preparedness Programs.

3. Provide knowledge base and support to apply technology to minimize and mitigate impacts of malicious plans and actions targeted at critical infrastructure systems.

- Identify and authenticate operators of critical infrastructure systems
- Provide physical security with sensors, alarms, and robots
- Ensure the availability of all network resources to protect against denial of service attacks
- Respond to security violations by notifying the proper authority, report forensic evidence of the violation in synthesized form, and automatically take timely corrective action in mission critical or safety critical situations
- Pursue, advocate, and actively adopt systems which provide inherent redundancy, confidentiality, and integrity
- Expand critical networks and systems with redundant architectures so that they can still operate in the event that a portion of the infrastructure is unavailable due to natural or human disasters
- Implement systems nationally so that there are no single points of failure
- Deploy information systems and networks so they are readily able to operate while receiving hostile traffic such as rapid unauthorized access attempts, viruses, worms, and denial of service attacks, without being infected or compromised and
- Promote that in system designs, always consider that a portion of the infrastructure may fail, due to human or natural causes. Plan for those contingencies and deploy infrastructure architectures which will inherently and dynamically respond and provide continued service in the event of a partial loss of the infrastructure.

4. Develop policies applicable to operators of critical infrastructure systems.

- Ensure that the physical plant of critical infrastructure systems is protected from illegal entry by malicious persons and damage by external forces (e.g., storms, lightning)
- Ensure that critical infrastructure systems are protected from chemical, biological, radiological, nuclear, and explosive attacks (e.g., poisoning of water supply, explosions, anthrax attacks, etc.)
- Ensure that the physical plants of critical infrastructure systems are protected from malicious/inadvertent damage by external forces (weather, lightning, flooding, et al) and intentional attack (chemical, biological, radiological, nuclear, and explosive, et al) and
- Recommend and provide best practices of jointly developed government/industry/professional society policies and practices that all critical infrastructure systems operators should utilize to protect their system.

The goal of protection must be to understand risks and contain, minimize, or prevent, the disruption of critical infrastructures by violent adversaries, malicious individuals, natural disasters, accidents, economic events, as well as create and recommend the methods for prevention, detection, or recovery from such events. Prevention efforts ideally devise protection measures consistent with risk.

This statement was developed by the IEEE-USA Critical Infrastructure Protection Committee and represents the considered judgment of a group of U.S. IEEE members with expertise in the subject field. IEEE-USA advances the public good and promotes the careers and public policy interests of more than 210,000 engineers, scientists and allied professionals who are U.S. members of IEEE. The positions taken by IEEE-USA do not necessarily reflect the views of IEEE or its other organizational units.