

Glossary of Key Terms

Many of the definitions in this Glossary are derived from language enacted in Federal laws and/or included in national plans, including the Homeland Security Act of 2002, USA PATRIOT Act of 2001, the National Incident Management System, and the National Response Plan.

All-Hazards. An approach for prevention, protection, preparedness, response, and recovery that addresses a full range of threats and hazards, including domestic terrorist attacks, natural and manmade disasters, accidental disruptions, and other emergencies.

Asset. Contracts, facilities, property, electronic and non-electronic records and documents, unobligated or unexpended balances of appropriations, and other funds or resources (other than personnel).

Business Continuity. The ability of an organization to continue to function before, during, and after a disaster.

Consequence. The result of a terrorist attack or other hazard that reflects the level, duration, and nature of the loss resulting from the incident. For the purposes of the NIPP, consequences are divided into four main categories: public health and safety, economic, psychological, and governance impacts.

Control Systems. Computer-based systems used within many infrastructure and industries to monitor and control sensitive processes and physical functions. These systems typically collect measurement and operational data from the field, process and display the information, and relay control commands to local or remote equipment or human-machine interfaces (operators). Examples of types of control systems include SCADA systems, Process Control Systems, and Digital Control Systems.

Critical Infrastructure. Assets, systems, and networks, whether physical or virtual, so vital to the United States that the incapacity or destruction of such assets, systems, or networks would have a debilitating impact on security, national economic security, public health or safety, or any combination of those matters.

Critical Infrastructure Information. Information not customarily in the public domain related to the security of

critical infrastructure or protected systems, and voluntarily provided to the government. CII includes any planned or past assessment, projection, estimate, operational problem, or solution regarding critical infrastructure or protected systems' ability to resist any actual, potential, or threatened unlawful interference with, attack on, compromise of, or incapacitation of this infrastructure or systems by either physical or computer-based attack.

Cyber Security. The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. Includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems.

Dependency. The one-directional reliance of an asset, system, network, or collection thereof, within or across sectors, on input, interaction, or other requirement from other sources in order to function properly.

Function. In the context of the NIPP, function is defined as the service, process, capability, or operation performed by specific infrastructure assets, systems, or networks.

Government Coordinating Council. The government counterpart to the SCC for each sector established to enable interagency coordination. The GCC is comprised of representatives across various levels of government (Federal, State, Territorial, local, and tribal) as appropriate to the security and operational landscape of each individual sector.

Hazard. Something that is potentially dangerous or harmful, often the root cause of an unwanted outcome.

Incident. An occurrence or event, natural or human-caused, that requires an emergency response to protect life or property. Incidents can, for example, include major disasters, emergencies, terrorist attacks, terrorist threats, wildland and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, and other occurrences requiring an emergency response.

Infrastructure. The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole. Consistent with the definition in the Homeland Security Act, infrastructure includes physical, cyber, and/or human elements.

Interdependency. The multi- or bi-directional reliance of an asset, system, network, or collection thereof, within or across sectors, on input, interaction, or other requirement from other sources in order to function properly.

Key Resources. As defined in the Homeland Security Act, “key resources” are publicly or privately controlled resources essential to the minimal operations of the economy and government.

Mitigation. Activities designed to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of an incident. Mitigation measures may be implemented prior to, during, or after an incident. Mitigation measures are often developed in accordance with lessons learned from prior incidents. Mitigation involves ongoing actions to reduce exposure to, probability of, or potential loss from hazards. Measures may include zoning and building codes, floodplain buyouts, and analysis of hazard-related data to determine where it is safe to build or locate temporary facilities. Mitigation can include efforts to educate governments, businesses, and the public on measures they can take to reduce loss and injury.

Network. In the context of the NIPP, a group of assets or systems that share information or interact with each other in order to provide infrastructure services within or across sectors.

Normalize. In the context of the NIPP, the process of transforming risk-related data into comparable units.

Owners/Operators. Those entities responsible for day-to-day operation and investment in a particular asset or system.

Preparedness. The range of deliberate critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents. Preparedness is a continuous process involving efforts at all levels of government and between government and private sector and nongovernmental organizations to identify threats, determine vulnerabilities, and identify required activities and resources to mitigate risk.

Prevention. Actions taken to avoid an incident or to intervene to stop an incident from occurring. Prevention involves actions taken to protect lives and property. Involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; immunizations, isolation, or quarantine; public health and agricultural surveillance and testing processes; and, as appropriate, specific law enforcement operations aimed at deterring, preempting, interdicting, or disrupting illegal activity and apprehending potential perpetrators and bringing them to justice.

Prioritization. In the context of the NIPP, prioritization is the process of using risk assessment results to identify where risk-reduction or mitigation efforts are most needed and subsequently determine which protective actions should be instituted in order to have the greatest effect.

Protection. Actions to mitigate the overall risk to CI/KR assets, systems, networks, or their interconnecting links resulting from exposure, injury, destruction, incapacitation, or exploitation. In the context of the NIPP, protection includes actions to deter the threat, mitigate vulnerabilities, or minimize consequences associated with a terrorist attack or other incident. Protection can include a wide range of activities, such as hardening facilities, building resiliency and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems, promoting workforce surety, and implementing cyber security measures, among various others.

Recovery. The development, coordination, and execution of service- and site-restoration plans for impacted communities and the reconstitution of government operations and services through individual, private sector, nongovernmental, and public assistance programs that identify needs and define resources; provide housing and promote restoration; address long-term care and treatment of affected persons; implement additional measures for community restoration; incorporate mitigation measures and techniques, as feasible; evaluate the incident to identify lessons learned; and develop initiatives to mitigate the effects of future incidents.

Resiliency. In the context of the NIPP, resiliency is the capability of an asset, system, or network to maintain its function during or to recover from a terrorist attack or other incident.

Response. Activities that address the short-term, direct effects of an incident, including immediate actions to save lives, protect property, and meet basic human needs.

Response also includes the execution of emergency operations plans and incident mitigation activities designed to limit the loss of life, personal injury, property damage, and other unfavorable outcomes. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into the nature and source of the threat; ongoing surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at preempting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.

Risk. A measure of potential harm that encompasses threat, vulnerability, and consequence. In the context of the NIPP, risk is the expected magnitude of loss due to a terrorist attack, natural disaster, or other incident, along with the likelihood of such an event occurring and causing that loss.

Risk Management Framework. A planning methodology that outlines the process for setting security goals; identifying assets, systems, networks, and functions; assessing risks; prioritizing and implementing protective programs; measuring performance; and taking corrective action. Public and private sector entities often include risk management frameworks in their business continuity plans.

Sector. A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society. The NIPP addresses 17 CI/KR sectors as defined in HSPD-7.

Sector Coordinating Council. The private sector counterpart to the GCCs, these councils are self-organized, self-run, and self-governed organizations that are representative of a spectrum of key stakeholders within a sector. SCCs serve as the government's principal point of entry into each sector for developing and coordinating a wide range of CI/KR protection activities and issues.

Sector Partnership Model. The framework used to promote and facilitate sector and cross-sector planning, coordination, collaboration, and information sharing for CI/KR protection involving all levels of government and private sector entities.

Sector-Specific Agency. Federal departments and agencies identified in HSPD-7 as responsible for CI/KR protection activities in specified CI/KR sectors.

Sector-Specific Plan. Augmenting plans that complement and extend the NIPP Base Plan and detail the application of the NIPP framework specific to each CI/KR sector. SSPs are developed by the SSAs in close collaboration with other security partners.

Security Partner. Those Federal, State, regional, Territorial, local, or tribal government entities, private sector owners and operators and representative organizations, academic and professional entities, and certain not-for-profit and private volunteer organizations that share in the responsibility for protecting the Nation's CI/KR.

Steady-State. In the context of the NIPP, steady-state is the posture for routine, normal, day-to-day operations as contrasted with temporary periods of heightened alert or real-time response to threats or incidents.

System. In the context of the NIPP, a system is a collection of assets, resources, or elements that performs a process that provides infrastructure services to the Nation.

Terrorism. Any activity that: (1) involves an act that is (a) dangerous to human life or potentially destructive of critical infrastructure or key resources, and (b) a violation of the criminal laws of the United States or of any State or other subdivision of the United States; and (2) appears to be intended to (a) intimidate or coerce a civilian population, (b) influence the policy of a government by intimidation or coercion, or (c) affect the conduct of a government by mass destruction, assassination, or kidnapping.

Threat. The intention and capability of an adversary to undertake actions that would be detrimental to CI/KR.

Value Proposition. A statement that outlines the national and homeland security interest in protecting the Nation's CI/KR and articulates benefits gained by all security partners through the risk management framework and public-private partnership described in the NIPP.

Vulnerability. A weakness in the design, implementation, or operation of an asset, system, or network that can be exploited by an adversary, or disrupted by a natural hazard or technological failure.

Weapons of Mass Destruction. (1) Any explosive, incendiary, or poison gas (i) bomb, (ii) grenade, (iii) rocket having a propellant charge of more than 4 ounces, (iv) missile having an explosive or incendiary charge of more than one-quarter ounce, or (v) mine or (vi) similar device; (2) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors; (3) any weapon involving a disease organism; or (4) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life (18 U.S.C. 2332a).