

Technology Letter (TL) 18-03
Recovery and Response Plans for Critical Infrastructure
Frequently Asked Questions

Question	Answer
<p>What is the process to identify critical infrastructure, consistent with SAM 5300.4?</p>	<p>As related to SAM 5300.4 further defining critical infrastructure may be considered in two complementary processes:</p> <ol style="list-style-type: none"> 1) Identification of organization mission essential functions that directly provide critical public services the disruption of which is evaluated as having a debilitating impact on public health, safety, economic security, or any combination thereof to the state. 2) Identification of critical physical infrastructure (such as dams, bridges, highways) the disruption of which is evaluated as having a debilitating impact on public health, safety, economic security, or any combination thereof to the nation or state that is under the operational control of the organization or over which the organization exercises oversight or regulatory authority.
<p>What criteria should be considered for identifying critical infrastructure?</p>	<p>Detailed criteria for recognition as mission essential functions and critical infrastructure vary. At a minimum the methodology for determining criticality should include an evaluation of both processes in the context of California’s State Essential Functions, and an evaluation of impacts on public health, safety, and economic security.</p>
<p>What are California State Essential Functions?</p>	<p>The California State Essential Functions are:</p> <ol style="list-style-type: none"> 1. Government Leadership – Provides visible and effective leadership for the people of California while restoring and maintaining critical state essential functions. 2. Public Safety – Maintains public safety and security for the people of California and decreases their vulnerability to threats and hazards. 3. Emergency Management – Protects and preserves the lives, property and environment for the people of California from the effects of natural, technological or human-caused disasters. 4. Public Health and Medical – Ensures the continuity and strength of California’s medical, public health, mental health organizations and systems. Supports the health and well-being of the people of California.

Technology Letter (TL) 18-03
Recovery and Response Plans for Critical Infrastructure
Frequently Asked Questions

	<p>5. Social Services and Education – Ensures the continuation of essential social services for the people of California, including services for vulnerable populations, victims of crime and special needs populations. Supports the continued operation of California’s educational systems (both public and private) at all levels of government.</p> <p>6. Critical Infrastructure – Preserves California’s infrastructure, including its transportation systems, energy systems, utilities, dams and other critical components. Supports and sustains the personnel required to operate and maintain the physical infrastructure.</p> <p>7. Financial, Economic and Business – Ensures the financial and economic security of California’s business, financial systems/institutions and its citizens. Preserves and supports California’s labor/workforce. Protects and preserves California’s tax and revenue collection capabilities to ensure continuity of California’s government.</p> <p>8. Information Technology/Communications – Protects, maintains and preserves California’s communications and technological capabilities. Ensures continued interoperability of California’s communications systems.</p> <p>9. Agriculture – Promotes and preserves the livelihood of California’s agricultural community and all its members. Ensures continuation of existing agriculture training and education programs. Ensures that California’s agriculture remains strong and competitive.</p> <p>10. Environment – Protects, preserves and restores California’s natural environment, ecosystems, resources and natural habitats and mitigates the impact of natural disasters or other events.</p> <p>11. Information Collaboration – Encourages and enhances information sharing and collaboration between Local/State/Federal and Private Sectors to more effectively respond and recover from all threats and protect the citizens of California.</p>
<p>Are there any guiding documents or supporting directives on critical infrastructure initiative?</p>	<p>The identification of critical physical infrastructure as defined in the Critical Infrastructures Protection Act of 2001, 42 U.S.C. 5195c(e) and Presidential Policy Directive (PPD) 21 on Critical Infrastructure Security and Resilience is divided into sixteen</p>

Technology Letter (TL) 18-03
Recovery and Response Plans for Critical Infrastructure
Frequently Asked Questions

	<p>sectors for the purpose of formalizing organizational responsibilities and focusing analytical efforts.</p> <p>Additional guiding documents include the U.S. National Infrastructure Protection Plan and Sector Specific Plans. Some sectors have published Sector Cybersecurity Frameworks.</p>
<p>Are there specific examples of critical infrastructure?</p>	<p>The following examples of simplified, primarily capacity-based criteria, are included for the purpose of illustrating possible approaches to identifying critical infrastructure and are neither exhaustive nor mandatory for use by state agencies:</p> <ol style="list-style-type: none"> 1. Chemical (Facilities with a current registered Risk Management Plan AND EITHER a total toxic chemical capacity of 500,000 lbs. or greater, OR an estimated population at risk of exposure within a 1-mile radius of 5,000 or greater.) 2. Commercial Facilities (Retail Facilities with an area greater than 1 million square feet and a capacity greater than 1,000 individuals, or if the facility is recognized both domestically and abroad as representing the Nation’s heritage, traditions, and/or values or is recognized for its national, commercial, cultural, historical, and/or civic significance.) 3. Communications (Major switching centers that support end users in excess of 150,000 people, and support a capacity in excess of 750,000 phone numbers.) 4. Critical Manufacturing (Single- or sole-source vendor that manufactures a product which is critical to California OR any manufacturer with an annual revenue in excess of \$1 billion.) 5. Dams and their control systems (Dams, navigation locks, levees, and flood control systems whose partial or total failure could be associated with a Population at Risk (defined as the population occupying permanent residences, commercial buildings, and recreational areas within potential zone of inundation represented by the dam-break flood scenario) of 1,000 people or more.) 6. Defense Industrial Base 7. Emergency Services (Multiagency coordination systems, mutual-aid systems, command-control-cyber intelligence-information technology (CCIIT) systems, and specialized emergency response systems, including key Emergency Operations Centers or dispatch centers whose exploitation or destruction would impact cities and/or incorporated areas with over 300,000 residents)

Technology Letter (TL) 18-03
Recovery and Response Plans for Critical Infrastructure
Frequently Asked Questions

	<ol style="list-style-type: none"> 8. Energy (All transmission substations along lines rated at 230 kV or higher that serve areas with a population of 50,000 persons or more. Operable petroleum refineries with refining capacity of 20,000 barrels per day or greater.) 9. Financial Services (Headquarters for commercial banks, credit unions, credit card companies, or financial holding companies (insurance, brokerage, and investment firms) with assets greater than \$10 billion.) 10. Food and Agriculture (Any pre-harvest facility (plant/crop or livestock operations) with a potential loss exceeding \$100 million (single catastrophic event), or assets producing greater than \$50 million of a product for which California produces 99% of the national total based on annual CDFA reporting.) 11. Government Facilities (Government owned or leased buildings, whether federal, state or local, that either have an occupancy of greater than 1,000 individuals.) 12. Healthcare and Public Health (General acute care hospital or acute psychiatric hospital facilities with a capacity of at least 500 beds.) 13. Information Technology (Information technology hardware manufacturers, software and application development firms, and information management solutions companies with annual revenue in excess of \$4 billion.) 14. Nuclear Reactors, Materials, and Waste (Research and Test Reactors employing highly enriched uranium.) 15. Transportation Systems (Highway tunnels and bridges that have annual average daily traffic (AADT) greater than 200,000 vehicles and a detour length greater than 1 mile.) 16. Water and Wastewater Systems [water supply, drinking water, waste water/sewage, stemming of surface water (e.g. dikes and sluices)] (Wastewater treatment facilities, wastewater collection systems and pumping systems (force mains), or wastewater storage system(s) that discharge greater than 200 KGD within 1 river miles of a water intake serving populations of 200,000 or more.)
<p>Are there any additional resources available?</p>	<p>The U.S. Department of Homeland Security , NIST Cybersecurity Framework, and Cal OES Continuity Planning Guidance provide additional information and guidance in this area.</p>