SAM 5300.4 Definitions - Revised and New

Term	Definition
Critical Infrastructure Controls	Networks and systems controlling assets so vital to the state that the incapacity or destruction of those networks, systems, or assets would have a debilitating impact on public health, safety, economic security, or any combination thereof. Source: Government Code Section 8592.30
Critical infrastructure information	Information not customarily in the public domain pertaining to any of the following: a) Actual, potential, or threatened interference with, or an attack on, compromise of, or incapacitation of critical infrastructure controls by either physical or computer-based attack or other similar conduct, including, but not limited to, the misuse of, or unauthorized access to, all types of communications and data transmission systems, that violates federal, state, or local law or harms public health, safety, or economic security, or any combination thereof. b) The ability of critical infrastructure controls to resist any interference, compromise, or incapacitation, including, but not limited to, any planned or past assessment or estimate of the vulnerability of critical infrastructure. c) Any planned or past operational problem or solution regarding critical infrastructure controls, including, but not limited to, repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to interference, compromise, or incapacitation of critical infrastructure controls. Source: Government Code Section 8592.30

Existing Definitions in SAM 5300.4 Definitions List

Critical Infrastructure	Critical infrastructure provides the essential services that underpin American society and serve as the backbone of our nation and state's economy, security, and health. Assets identified as essential to the state, U.S. society and the economy, public health, safety, economic security, or any combination thereof. These include, as examples, facilities, systems and services within the following sectors: 1. Chemical 2. Commercial Facilities 3. Communications (telecommunications) 4. Critical Manufacturing 5. Dams and their control systems

	6. Defense Industrial Base (police, military) 7. Emergency Services (first responders, police, military) 8. Energy [electricity generation, transmission and distribution; gas production, transport and distribution; and oil and oil products production, transport and distribution; heating (e.g. natural gas, fuel oil, district heating)] 9. Financial Services (banking, clearing) 10. Food and Agriculture (agriculture, food production and distribution) 11. Government Facilities 12. Healthcare and Public Health (hospitals, ambulances) 13. Information Technology 14. Nuclear Reactors, Materials, and Waste 15. Transportation Systems (fuel supply, railway network, airports, ports, harbors, inland shipping) 16. Water and Wastewater Systems [water supply, drinking water, waste water/sewage, stemming of surface water (e.g. dikes and sluices)] Sources: U.S. Department of Homeland Security and Critical Infrastructures Protection Act of 2001, 42 U.S.C. 5195c(e) Note: See Critical Infrastructure FAQ for further assistance with the process of identifying critical infrastructure.
Information Technology Infrastructure	An agency's information technology platform for the support of agency programs and management. Included in the infrastructure are equipment, software, communication networks. Source: SAM Section 4989.1
Risk Analysis	The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment. Source: SAM 5300.4, Definitions based on NIST Glossary of Key Information Security Terms
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation, arising through the operation of an asset. Part of risk management, incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis. Source: SAM 5300.4, Definitions based on NIST Glossary of Key Information Security Terms