Supply Chain Risk Management (SCRM) ICT Supplier Risk Management Standard Definitions

Number	*Term*	*Definition*	*Source*
1.	Bad Actors/Malicious Actors	Individual, organization, or nation-state who "touch" a product, direct or indirect, to affect the management or operations of companies that may result in compromise to the information system, organization, or Nation.	NIST IR 7622, Notional Supply Chain Risk Management Practices for Federal Information Systems, Page 14.
2.	Counterfeit	Unauthorized modification, diversion, or unauthorized substitution of genuine parts.	Key Practices and Implementation Guide for the DoD Comprehensive National Cybersecurity Initiative 11 Supply Chain Risk Management Pilot Program, Page 20.
3.	Critical Component	A component which is or contains ICT, including hardware, software, and firmware, whether custom, commercial, or otherwise developed, and which delivers or protects mission critical functionality of a system or which, because of the system's design, may introduce vulnerability to the mission critical functions of an applicable system.	DODI 5200.44, November 5, 2012, Glossary, Part II, Definitions, Page 11.
4.	Cyber Warfare	Cyber warfare involves nation-states using information technology to penetrate another nation's networks to cause damage or disruption.	Next-Generation Network Security, link: http://www.paloaltonetworks.com/community/learning-center/what-is-cyber-security.html

Number	*Term*	*Definition*	*Source*
5.	ICT – Information and Communications Technology	Includes all categories of ubiquitous technology used for gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks).	DODI 5200.44, November 5, 2012, Glossary, Part II, Definitions, Page 12.
6.	ICT Supply Chain	Globally distributed, interconnected set of organizations, people, processes, products, and services.	NIST IR 7622, Notional Supply Chain Risk Management Practices for Federal Information Systems; Introduction, page 9.
7.	Insider Threat	Includes concerning behaviors such as inordinate, long-term job dissatisfaction, attempts to gain access to information not required for job performance, unexplained access to financial resources, bullying or sexual harassment of fellow colleagues, workplace violence, and other serious violations of organizational policies, procedures, directives, rules, and/or practices.	NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, Page F-32.
8.	Malicious hardware	A virus or other malicious software that is attached to a program preloaded on a computer or external hard drive. A CPU chip in a computer or handheld device that has a built-in back door, enabling an attacker to gain illegal entrance.	The Free Dictionary, link: http://encyclopedia2.thefreedictionary.com/malicious+hardware

Number	*Term*	*Definition*	*Source*
9.	Nation State	A form of political organization in which a group of people who share the same history, traditions, or language live in a particular area under one government.	http://www.learnersdictionary.com/search/nation-state
10.	Software /Malicious Code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.	NIST SP 800-53, Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations, Page B-10.
11.	Spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code	NIST SP 800-53, Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations, Page B-19.
12.	Terrorist Organization	Any number of terrorists who assemble together, have a unifying relationship, or are organized for the purpose of committing an act or acts of violence or threatens violence in pursuit of their political, religious, or ideological objectives.	http://wstiac.alionscience.com/pdf/dodmilitarydictionary.pdf