



SUSTAINMENT

ASSISTANT SECRETARY OF DEFENSE
3500 DEFENSE PENTAGON
WASHINGTON, DC 20301-3500

NOV 28 2022

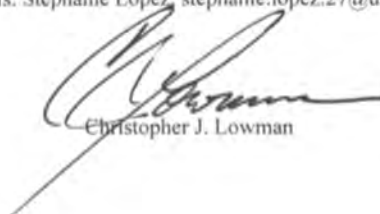
MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Supply Chain Risk Management Draft Taxonomy Version 1.0 – Advance Copy

As the Department of Defense (DoD) proponent for development and implementation of supply chain risk management (SCRM) policies, in May 2022, my office initiated a project to develop a common SCRM framework and taxonomy in coordination with DoD components, interagency partners, academia, industry, and standards bodies. While we continue to develop and coordinate the common framework, which will clearly identify SCRM roles and responsibilities across the DoD, we have completed the development of a draft SCRM Taxonomy Version 1.0, detailed in the attachment, consisting of 12 risk categories and 124 sub-risk categories. In addition, the Taxonomy includes proposed definitions for Supply Chain Resilience, SCRM, and Supply Chain Security.

I am providing an advance copy of the draft SCRM Taxonomy Version 1.0 to facilitate the communication of risk information across the DoD. Many DoD Components are currently using the Taxonomy to assess and categorize risks, to include incorporating the taxonomy into information technology systems, databases, programs, policies, and processes. My office will officially publish the Taxonomy as part of a new SCRM DoD Instruction, with estimated publication planned for early Fiscal Year 2024.

Your organizations have been instrumental in completing the draft SCRM Taxonomy Version 1.0 and I greatly appreciate your ongoing support as we develop and refine it as well as other key products for management of the risks within the DoD supply chain. My points of contact for this effort are BG Michelle Link, michelle.a.link2.mil@mail.mil; Mr. Jared Andrews, jared.m.andrews6.ctr@mail.mil; and Ms. Stephanie Lopez, stephanie.lopez.27@us.af.mil.



Christopher J. Lowman

Attachment:
As stated

Definitions

Terms	Proposed definitions
Supply Chain Resilience (SCR)	The capability of supply chains to respond quickly, so as to ensure continuity of operations after a disruption, and to quickly adapt to change. Resilience is the expected outcome of proactive Supply Chain Risk Management and Supply Chain Security.
Supply Chain Risk Management (SCRM)	The process of proactively identifying supply chain vulnerabilities, threats, and potential disruptions and implementing mitigation strategies to ensure the security, integrity, and uninterrupted flow of materials, products, and services as risks are found or disruptions occur.
Supply Chain Security (SCS)	The application of policies, procedures, processes, and technologies to ensure the security, integrity, and uninterrupted flow of products while moving through the supply chain. Examples include the ability to protect supply chains from cyber infiltrations and the introduction of counterfeit material.

Risks

Risk category	Proposed definitions
Foreign Ownership Control or Influence (FOCI)	A company is considered to be operating under FOCI whenever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable, to direct or decide matters affecting the management or operations of that company in a manner which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts and/or programs which support national security.
Political & Regulatory	The weakness of the political powers and their legitimacy and control. Inadequacy of the control schemes, policies and planning, or broad political conditions. Includes terrorism, government policy changes, systematic corruption, and energy crises in the international marketplace. This can occur when changes in laws or regulations materially impact a security, business, sector or market. New laws and regulations enacted by the government or regulatory body can increase costs of operating a business, reduce the attractiveness of investment, or change the competitive landscape. Includes issues such as civil unrest or conflict and acts of terrorism that negatively impact supply chain operations. A certified act of terrorism must fall within the four identified descriptors determined by the Terrorism Risk Insurance Act (TRIA) and the Secretary of Treasury.
Economic	Currency fluctuations, instability in demand and prices, changing labor costs and inflationary pressures present challenges for suppliers to accurately plan their investment in foreign markets.
Environmental	Include natural and manmade disasters that may disrupt supply chains. Natural disasters and other extreme weather conditions comprise the bulk of external environmental risk. Manmade disasters can arise from improper health and safety, fires, spills, chemical leaks, and other environmental hazards.
Product Quality & Design	Occurs due to inherent design and quality problems (e.g., raw materials, ingredients, production, logistics, packaging) in which the part does not meet performance specifications and quality standards set by industry or DoD. Includes the detection of a part that was illegally created and sold under false pretenses. The part has not faced industry standard tests during the production phase (e.g., pressure testing) to ensure sustainability during usage. Counterfeit and non-MILSPEC parts pose significant risk to the function and safety of the system through malicious intrusion via backdoor exposures; increased maintenance costs due to depreciation in quality; and added stresses due to the parts inability to function at true capacity.
Manufacturing & Supply	Occurs when a supplier cannot fulfill the supply of a product to meet market demand. This can be due to reduced throughput or production delays caused by equipment down-time, capacity constraints, and delays in material delivery. Additional concerns include availability of supply, sole-source, and concentration within a singular country creating over-reliance.

Risk category	Proposed definitions
Transportation & distribution	Occurs when there is a dynamic disruption within the transportation and logistics of a product from one point to another. The transportation industry is among the most risk-prone of all industries, due to accidents, losses of cargo, driver shortages, and deteriorating infrastructure. These risks can cause shipment delays, supply chain disruptions, increased costs, and damaged reputations. In addition, the inability to predict and plan for disruptions in the logistics plan presents risk in meeting delivery requirements and maintaining operations.
Financial	The condition in which a supplier cannot generate revenue or income resulting in the inability to meet financial obligations. This is generally due to high fixed costs, illiquid assets, or revenues sensitive to economic downturns. Financial distress can lead to the inability to meet contractual obligations, hostile takeovers, or bankruptcy.
Compliance	Inability to comply with a wide-arching set of guidelines, policies, laws, and/or agreements established to avoid impact to national security.
Technology & Cyber Security	Involves the management of cybersecurity requirements for information technology systems, software and networks, which are driven by threats such as cyber-terrorism, malware, data theft and the advanced persistent threat (APT). Technology risks include vulnerabilities and exposures of systems components and information systems produced by a specific supplier. Common risks include weaknesses in computation logic (code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity or availability.
Human Capital	Associated with human skills, knowledge and ethical conduct of an organization, including industrial disputes and labor unrest.
Infrastructure	Infrastructure required to support supply chains within a country (e.g., buildings, water, electricity, roads).

Sub-Risk Categories

Risk sub-categories	Proposed definitions
Risk category: Compliance	
Trafficking in Persons	“Trafficking in persons,” “human trafficking,” and “modern slavery” are umbrella terms – often used interchangeably – to refer to a crime whereby traffickers exploit and profit at the expense of adults or children by compelling them to perform labor or engage in commercial sex.
SEC Enforcement Action	Actions that take place by the SEC to address misconduct that arose from or led to financial crimes.
Past suspension or Debarment	Suspend - to temporarily pause or delay work with the option to continue later. This action must be taken by a suspending official and executed in accordance with FAR 9.4. Debar - to disqualify the person or company from receiving contracts. Must be completed by a debarring official and executed in compliance with FAR 9.4.
Occupational Workers Health and Safety (OSHA)	Safe and healthful working conditions for workers by setting and enforcing standards and by providing training, outreach, education and assistance.
Risk category: Compliance (continued)	
Legal and Reputational	Examples include lawsuits, discrimination, and other law enforcement actions.

Risk sub-categories	Proposed definitions
Insider Threat	Insider threat is the potential for an insider to use their authorized access or understanding of an organization to harm that organization.
Import/Export Violation	Both the deliberate and non-deliberate violation of the customs laws of the United States.
Human Rights	Rights regarded as belonging fundamentally to all persons (e.g., freedom from unlawful imprisonment, torture, and execution).
Fraud (Procurement and Government)	<p>Fraudulent activities by Federal or State employees, contractors, subcontractors, or any other participants on government contracts. Suspected fraudulent activities include, but are not limited to:</p> <ul style="list-style-type: none"> falsifying information on contract proposals using Federal funds to purchase items that are not for Government use billing more than one contract for the same work billing for expenses not incurred as part of the contract billing for work that was never performed, falsifying data substituting approved materials with unauthorized products misrepresenting a project's status to continue receiving Government funds charging higher rates than those stated or negotiated for in the bid or contract influencing government employees to award a grant or contract to a particular company, family member, or friend.
Forced Labor	Forced labor occurs when individuals are compelled to provide work or service through the use of force, fraud, or coercion.
Ethics Violation	A violation of moral principles that govern a person's behavior or the conducting of an activity.
Defective Pricing	Result of Cost/Pricing Data (C/PD) that was certified by a contractor to be accurate, current, and complete but was not.
Contractor Misconduct	When companies that sell goods or services to the government violate laws or regulations or are the subject of misconduct allegations in their dealings with the government, individuals, or private entities.
Contract Non-Compliance	Non-compliance occurs when one party in a contract does not fulfill his or her obligations.
Conflict Minerals and Raw Materials in Supply Chain	Natural resources extracted in a conflict zone. In the United States, companies must report on their use and sourcing of tin, tantalum, tungsten and gold and raw materials.
Anti-trust / Monopolistic Practices	<p>Practices that unduly restrain competitive trade.</p> <p>Monopolistic practices - Companies' actions to create a monopoly. A monopoly refers to when a company and its product offerings dominate a sector or industry. Monopolies can be considered an extreme result of free-market capitalism in that, absent any restriction or restraints, a single company or group becomes large enough to own all or nearly all of the market (goods, supplies, commodities, infrastructure, and assets) for a particular type of product or service. The term monopoly is often used to describe an entity that has total or near-total control of a market.</p>

Risk sub-categories	Proposed definitions
Risk category: Economic	
Recession, Economic Slowdown	A period of temporary economic decline during which trade and industrial activity are reduced, generally identified by a fall in GDP in two successive quarters.
Price Volatility/Market Risk	The sensitivity of the financial institution's earnings or the economic value of its capital to adverse changes in interest rates, foreign exchanges rates, commodity prices, or equity prices.
Inflation	Inflation is the increase in the prices of goods and services over time.
High Unemployment	The term unemployment refers to a situation where a person actively searches for employment but is unable to find work. Unemployment is considered to be a key measure of the health of the economy.
Economic Sanctions	Economic sanctions are defined as the withdrawal of customary trade and financial relations for foreign- and security-policy purposes. Sanctions may be comprehensive, prohibiting commercial activity with regard to an entire country, like the long-standing U.S. embargo of Cuba, or they may be targeted, blocking transactions by and with particular businesses, groups, or individuals.
Economic instability	Economic instability occurs when the factors that influence an economy are out of balance. When an economy becomes unstable, there is inflation, which is a decrease in the value of money. This leads to higher prices, higher unemployment rates, and general angst among consumers and businesses that are trying to survive financially. Causes of economic instability: stock market fluctuations, fall in home prices, interest rate changes, black swan events (hurricane, terrorist attack, etc.)
Demand Shocks	A demand shock is a sudden unexpected event that dramatically increases or decreases demand for a product or service, usually temporarily.
Currency Fluctuations	Currency fluctuations are a natural outcome of floating exchange rates, which is the norm for most major economies. Numerous factors influence exchange rates, including a country's economic performance, the outlook for inflation, interest rate differentials, capital flows and so on. A currency's exchange rate is typically determined by the strength or weakness of the underlying economy. As such, a currency's value can fluctuate from one moment to the next.
Risk category: Environmental	
Wildfire	A large, destructive fire that spreads quickly over woodland or brush.
Pandemic	A pandemic is the worldwide spread of a new disease.
Natural Disaster	Natural disasters include all types of severe weather, which have the potential to pose a significant threat to human health and safety, property, critical infrastructure, and homeland security. Natural disasters occur both seasonally and without warning, subjecting the nation to frequent periods of insecurity, disruption, and economic loss.
Man-made Risk	The exposure to dangerous or harm as a result of human intent, negligence, or error involving a failure of a man-made process or system, as opposed to natural disasters resulting from natural hazards.

Risk sub-categories	Proposed definitions
Risk category: Environmental (continued)	
Extreme Weather Event	Refers to weather phenomena that are at the extremes of the historical distribution and are rare for a particular place and/or time, especially severe or unseasonal weather. Such extremes include severe thunderstorms, severe snowstorms, ice storms, blizzards, flooding, hurricanes, and high winds, and heat waves. For example, although flooding is common in the United States, the impacts of flooding are not consistent from year to year through time. Many years of small floods with little impact may be followed by a single large flood with a sizable loss.
Climate	The impact that adverse climate-related conditions can impact the supply chain.
Chemical Spill (Hazmat)/chemical, biological, radiological, or nuclear incident	Chemical spills are the uncontrolled release of a hazardous chemical, either as a solid, liquid or a gas. Any occurrence, resulting from the use of chemical, biological, radiological, and nuclear weapons and devices; the emergence of secondary hazards arising from friendly actions; or the release of toxic industrial materials or biological organisms and substances into the environment, involving the emergence of chemical, biological, radiological, and nuclear hazards.
Risk category: Financial	
Unstable Payment Performance	When a company does not consistently "transfer money, goods or services in exchange for goods and services in acceptable proportions that have been previously agreed upon by all parties involved".
Solvency, Credit Risk	Solvency is the ability of a company to meet its long-term debts and financial obligations. Solvency can be an important measure of financial health, since its one way of demonstrating a company's ability to manage its operations into the foreseeable future. The quickest way to assess a company's solvency is by checking its shareholders' equity on the balance sheet, which is the sum of a company's assets minus liabilities.
Profitability Measures	Profitability ratios are a class of financial metrics that are used to assess a business's ability to generate earnings relative to its revenue, operating costs, balance sheet assets, or shareholders' equity over time, using data from a specific point in time.
Operational Efficiency Risk	<p>In a business context, operational efficiency is a measurement of resource allocation and can be defined as the ratio between an output gained from the business and an input to run a business operation. When improving operational efficiency, the output to input ratio improves.</p> <p>Operational risk summarizes the uncertainties and hazards a company faces when it attempts to do its day-to-day business activities within a given field or industry. A type of business risk, it can result from breakdowns in internal procedures, people and systems—as opposed to problems incurred from external forces, such as political or economic events, or inherent to the entire market or market segment, known as systematic risk.</p> <p>Operational risk can also be classified as a variety of unsystematic risk, which is unique to a specific company or industry.</p>
Offshore Leaks/Database	The ICIJ Offshore Leaks Database represents a large set of relationships between people, companies, and organizations involved in the creation of offshore companies in tax-heaven territories, mainly for hiding their assets.

Risk sub-categories	Proposed definitions
Risk category: Financial (continued)	
Liquidity Risk	The risk of incurring losses resulting from the inability to meet payment obligations in a timely manner when they become due or from being unable to do so at a sustainment cost
Lack of Funding Sources	(1) Funding is money which a government or organization provides for a particular purpose. If sufficient funding is unavailable, it will limit the provider’s ability to meet requirements. (2) An absence or limit in the assortment of capital a business can access to reinvest into business operations.
Financial Crimes	Financial crime refers to all crimes committed by an individual or a group of individuals that involve taking money or other property that belongs to someone else, to obtain a financial or professional gain.
Dependence on Defense Contracts	Consider DoD sales relative to total global sales for the facility. "Mixed" market is ~50% DoD; "Significant" is ~>60% for DoD or >60% for non-DoD; Very Strong or very weak DoD dominance can be risky for different reasons: High dependence on DoD contracts makes a facility more susceptible to DoD funding decisions. Low dependence on contracts makes the DoD more susceptible to business decisions by the facility.
Cyclical Risk	Cyclical risk is the risk of business cycles or other economic cycles adversely affecting the returns of an investment, an asset class or an individual company's profits.
Costs Overruns	A cost overrun, also known as a cost increase or budget overrun, involves unexpected, incurred costs. When these costs are in excess of budgeted amounts due to a value engineering underestimation of the actual cost during budgeting, they are known by these terms. Cost overruns are common in infrastructure, building, and technology projects and Weapon Systems.
Bankruptcy	The state of being completely lacking particular quality or value.
Risk category: FOCI	
Weaponized Mergers and Acquisitions (M&A)	The use by national governments of the tools of regulation of M&A to advance, explicitly or implicitly, domestic political and trade agendas.
Veiled Venture	An acquisition or economic-related action designed to camouflage nefarious intent of an individual, company, or country.
Theft of Trade Secrets	Trade secrets are a type of intellectual property that comprise formulas, practices, processes, designs, instruments, patterns, or compilations of information that have inherent economic value because they are not generally known or readily ascertainable by others, and which the owner takes reasonable measures to keep secret. In some jurisdictions, such secrets are referred to as confidential information.
State-owned Company	A state-owned enterprise (SOE) is a legal entity that is created by a government in order to partake in commercial activities on the government’s behalf. A state-owned enterprise or government-owned enterprise is a business enterprise where the government or state has significant control through full, majority, or significant minority ownership.

Risk sub-categories	Proposed definitions
Risk category: FOCI (continued)	
Sabotage	1: destruction of an employer's property (such as tools or materials) or the hindering of manufacturing by discontented workers 2: destructive or obstructive action carried on by a civilian or enemy agent to hinder a nation's war effort 3a: an act or process tending to hamper or hurt 3b: deliberate subversion
Provenance	The extent to which a supplier relies on parts that are manufactured, sold, or distributed by companies that have part or whole foreign ownership or significant foreign influence.
Partnership with State-owned Entity	A state-owned enterprise (SOE) or government-owned enterprise (GOE) is a business enterprise where the government or state has significant control through full, majority, or significant minority ownership. Defining characteristics of SOEs are their distinct legal form and operation in commercial affairs and activities. While they may also have public policy objectives (e.g., a state railway company may aim to make transportation more accessible), SOEs should be differentiated from government agencies or state entities established to pursue purely nonfinancial objectives.
Nationalization	A national government can transform privately-owned businesses into state-owned businesses, which can enable foreign governments to enter existing supply chains.
Industrial Espionage	Industrial espionage, economic espionage, corporate spying or corporate espionage is a form of espionage conducted for commercial purposes instead of purely national security. While economic espionage is conducted or orchestrated by governments and is international in scope, industrial or corporate espionage is more often national and occurs between companies or corporations.
Foreign Intelligence Entity (FIE)	Any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. The term includes foreign intelligence and security services and international terrorists.
Executive Poaching	The intentional action of one company to hire an employee or group of employees currently employed at another company (many times a competing company).
Cyber Espionage	Cyber espionage is a form of cyber-attack that steals classified, sensitive data or intellectual property to gain an advantage over a competitive company or government entity.
Counterintelligence	Information gathered, and activities conducted to detect, identify, exploit and neutralize the intelligence capabilities and activities of terrorists, foreign powers and other entities directed against US national security.
CI Collection	The systemic acquisition of intelligence information to answer CI collection requirements.
CI Analysis	The process of examining and evaluating raw information to determine the nature, function, interrelationships, personalities, and intent regarding the intelligence capabilities of a foreign intelligence entity (FIE).

Risk sub-categories	Proposed definitions
Risk category: Human Capital	
Work Stoppage	A cessation of work by employees as a job action. Work stoppage is often used to refer to a cessation of work that is less serious and more spontaneous than one referred to as a strike.
Loss of Talent/Skill, Mass Lay-offs	An absence or decline in workforce knowhow resulting in diminished domestic capabilities.
Lack of Access to Capable Workforce/Labor Shortages	When a labor shortage occurs, it means that employers are having a difficult time recruiting qualified applicants for available job openings. There are not enough candidates to fill the roles employers are hiring for or there only a few available candidates and are hard to find.
Labor Dispute	The term “labor dispute” includes any controversy concerning terms, tenure or conditions of employment, or concerning the association or representation of persons in negotiating, fixing, maintaining, changing, or seeking to arrange terms or conditions of employment, regardless of whether the disputants stand in the proximate relation of employer and employee.
Boycotts	Withdraw from commercial or social relations with (a country, organization, or person) as a punishment or protest
Risk category: Infrastructure	
Utilities	Any and all utility services and installations including, but not limited to, gas, water, electricity, telephone, other telecommunications, steam, sewer and storm sewer, and all piping, wiring, conduit and/or other fixtures related thereto or used in connection therewith. To include Water – includes the material and availability therein of irrigation, sanitation, production and transportation (see waterway) of material and/or products. Water Supply sources and their surroundings from which water is supplied for drinking, manufacturing, production, industrial, or domestic purposes.
Security	<ol style="list-style-type: none"> 1. Measures taken by a military unit, activity, or installation to protect itself against all acts designed to, or which may, impair its effectiveness. (JP 3-10) 2. A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. (JP 3-10) 3. With respect to classified matter, the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security.
Roads, Rail, Water etc.	<p>Railroads are of particular importance for the movement of commodities that are heavy and moved in bulk over long distances. This also includes the use of water as a mode of transportation and roadways in and out of industrial facilities.</p> <p>Waterway – a river, canal, or other body of water serving as route or way to travel or transport.</p>
Equipment	Equipment — In logistics, all nonexpendable items needed to outfit or equip an individual or organization. See also component, supplies. (JP 4-0)

Risk sub-categories	Proposed definitions
Risk category: Infrastructure (continued)	
Energy Scarcity	Energy scarcity - any significant bottleneck in the supply of energy resources to manufacturing, production, or economy. Additionally, in economics, a commodity is called scarce if using that commodity in one specific way implies that it can no longer be used in any other way.
Building/Facilities conditions	<p>Facility — A real property entity consisting of one or more of the following: a building, a structure, a utility system, pavement, and underlying land. (JP 3-34).</p> <p>Building conditions- the state of facilities and buildings measured through various metrics such as Building Condition Index (engineering assessment) or Facilities Condition Index (cost of repair divided by cost of replacement). Generally, the lower the score the lower the quality of building and expected storage capabilities and productive output.</p>
Risk Category: Manufacturing and Supply	
Underdeveloped Product Pipeline	Used to transmit fuel and natural gas or derivatives to manufacturing and supply facilities. The extent to which the OEM is resilient to delays in supply chain capacity and development needed to meet extant and nascent manufacturing requirements
Throughput/Production Delays	A delay in the amount of a product or service that a company can produce and deliver to a client within a specified period of time.
Sole Source Dependency	Only one supplier for the required item is available.
Single Source	A particular supplier is purposefully chosen by the buying organization, even when other suppliers are available
Reseller/3rd Party Vendor/Middleman	A person or company that sells something they have bought from someone else.
Reclamation/Utilization	Process to reclaim whole or essential components and materials for manufacturing either the same or alternate products. Reutilization is using components and materials for the same, similar, or differing purpose (e.g., using ships again in different missions or sinking to build reefs)
Parts/Spares Inventory Shortages	Inadequate supplies of spare parts on hand for maintenance and repairs.
Outsourcing	Outsourcing is the business practice of hiring a party outside a company to perform services and create goods that traditionally were performed in-house by the company's own employees and staff.
Order Fulfillment	The complete process from point of sales inquiry to delivery of a product to the customer.
Material Sources	The origin of materials which have been used to form or manufacture a product generally represented as the N-1 Supply Tier. This includes direct material used in the product and indirect material used in production and manufacturing, e.g., castings.

Risk sub-categories	Proposed definitions
Risk category: Manufacturing and Supply (continued)	
Inventory Stockout/Material Shortages	A stockout, or out-of-stock (OOS) event is an event that causes inventory to be exhausted.
Inventory or Capacity Incidents	Loss of inventory or capacity from events. This may be a loss from building failure, access restrictions, etc.
Industrial Capacity	Industrial capacity is “the amount (e.g., quantity) of industrial capability” or “the amount (e.g., quantity) of the ability of industry to accomplish a result”. This could include products (e.g., industry can make one item per month with existing lines), services (e.g., industry can service one plane per hour), and changes (e.g., if industry received \$XX this month they could increase by YY production lines next month to make 50 items per month).
Industrial Capability	Industrial capability is “the ability of industry to accomplish (make, create, destroy, etc.) a result (product, information, objective, etc.)” This drives both the larger products (e.g., can we make airplanes?) and more specifics (e.g., can we make a stealth covering for legacy airplanes to avoid aerial reconnaissance while on the tarmac?)
Extended Lead Times	Unplanned and/or unexpected time it takes between order initiation and product delivery.
Equipment Down Time	Equipment downtime refers to the amount of time that equipment is not operating, whether that is a result of unplanned equipment failure (e.g., a fault or broken part) or planned downtime (e.g., necessary downtime for preventive maintenance).
Obsolescence/DMSMS	Obsolescence is defined as the loss or impending loss of original manufacturers of items or suppliers of items or raw materials. This type of obsolescence is commonly referred to as DMSMS (Diminishing Manufacturing Sources and Material Shortages) within the Department of Defense, which is caused by the unavailability of technologies or parts that are necessary to manufacture or sustain a system. Due to the length of the system’s manufacturing and support life, and unforeseen life extensions to the support of the system longer than its planned end of support date, the parts and other resources necessary to support the system become unavailable before the system’s demand for the parts or other resources ends.
Concentration Risk	The probability of loss likely to arise due to over-dependence on a single vendor, concentration risk is further exacerbated when such a vendor specializes in a specific industry.
Agriculture	Agriculture is the art and science of cultivating the soil, growing crops and raising livestock. It includes the preparation of plant and animal products for people to use and their distribution to markets. Agriculture provides most of the world's food and fabrics.
Adjacency Risk	When separate industries (e.g. auto industry and defense sector) compete for limited resources (e.g., microchips).

Risk sub-categories	Proposed definitions
Risk category: Political and Regulatory	
Watch List	The watchlist is used by government agencies with a national security mission to support: Visa and passport screening (Department of State), International travel into the U.S. (U.S. Customs and Border Protection), and air passenger screening for terrorism (Transportation Security Administration).
Trade Wars	Trade war happens when one country retaliates against another by raising import tariffs or placing other restrictions on the other country's imports.
Terrorism	The unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives
Territorial Disputes on trade routes	A trade route is a logistical network identified as a series of pathways and stoppages used for the commercial transport of cargo. Territorial disputes involve disagreement about who controls a particular territory or trade route.
Political/Government Changes	The risk that political changes or instability in a country could pose to a supply chain. Instability could stem from a change in government, legislative bodies, other foreign policymakers or military control. Political risk is also known as "geopolitical risk," and becomes more of a factor as the time horizon of investment gets longer. Government risk manifests when the actions of government increase uncertainty with respect to an organization, project or activity. An example of government risk is when poor behavior of an industry or sector leads to a government policy or regulatory response.
Interstate conflict (War or Armed Conflict)	Interstate conflict involves violence between two or more states.
Government Policies	All DoD Polices/Regulations such as: DoD Acquisition process, DoD Acquisition and Supply regulations, Intel, Information Technology, Industrial Base, Domestic and global transportation regulations
Government Collapse	State collapse, breakdown, or downfall is the complete failure of a mode of government within a sovereign state.
Exposure (Potential Political)	The condition of being exposed to several events: such as: <ul style="list-style-type: none"> ● the condition of being presented to view or made known ● the condition of being unprotected especially from severe weather ● the condition of being subject to some effect or influence ● the condition of being at risk of financial loss
Environmental Protection Agency (EPA)	The mission of EPA is to protect human health and the environment.
Corruption	Corruption is dishonest behavior by those in positions of power, such as managers or government officials. Corruption can include giving or accepting bribes or inappropriate gifts, double-dealing, under-the-table transactions, manipulating elections, diverting funds, laundering money, and defrauding investors.
New Regulations, Changes in Policy (e.g., Trade Policy)	Changes in government policies or regulations that impact the supply chain.
Border Delays	Border delays can result in the timely delivery of materials/items.

Risk sub-categories	Proposed definitions
Risk category: Product Quality & Design	
Unreported Supplier Recalls	Unsupported Product Recall means recalls unsubstantiated by documentation or receipts incurred by third parties selling a Product(s) that is included in a Recall(s) to the end user(s).
System/Parts Performance Failure	Performance is a measurement of either work or time, for example, system-related work accomplished within a given time and the time required to complete a task or job, based upon past performance.
Product Characteristics	Product characteristics can inform decisions on whether products can be interchangeable or substitutable.
Non-MILSPEC Parts	Non-MILSPEC parts items may not conform to military specifications and could result in product failure.
Non-Conforming Parts	Non-conforming materials are any product or parts that are defective, counterfeit or do not meet the requirements.
Counterfeit Parts	The unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified item from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitution includes used items represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.
Risk category: Technology and Cyber Security	
Unsecure Networks or Systems	An unsecured network or system lacks intrusion detection and prevention capability.
OPSEC / INFOSEC Violation	<p>OPSEC (operational security) is an analytical process that classifies information assets and determines the controls required to protect these assets.</p> <p>After vulnerabilities have been determined, the next step is to determine the threat level associated with each of them. OPSEC encourages managers to view operations or projects from the outside-in, or from the perspective of competitors (or enemies) in order to identify weaknesses. If an organization can easily extract their own information while acting as an outsider, odds are adversaries outside the organization can as well. Completing regular risk assessments and OPSEC is key to identifying vulnerabilities.</p>
Malicious Intrusion	Intrusions that take place anytime a bad actor gains access to an application with the intent of causing harm to or steal data from the network or user.
Loss or Theft Of DCI/PII Discharge of Classified Information = DCI; Personally Identifiable Information = PII	<p>PII—The removal or unlawful taking of information that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors.</p> <p>CII—The removal or unlawful taking of information that a defense organization has determined to be valuable to an adversary. This information may vary based on the organization’s role.</p>

Risk sub-categories	Proposed definitions
Risk category: Technology and Cyber Security (continued)	
IT Obsolescence	When a technical product or service is no longer needed or wanted even though it could still be in working order. Technological obsolescence generally occurs when a new product has been created to replace an older version.
IT Implementation Failure	A new system implementation or upgrade that fails to a degree where normal business operations are negatively impacted
IT Disruption/Connectivity Issues	An IT issue that disrupts normal business operations such as an outage, errors while implementing new technology, ransomware, or IT overloads
Data Breach	A data breach is a security violation, in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.
Cyber Attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure, or destroying the integrity of the data or stealing controlled information.
Critical Hardware/Software Vulnerability	A weakness in automated system security procedures, administrative controls, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.
Risk Category: Transportation and Distribution	
Transportation Network Disruption	Disruptions to the transportation network can cause delays or missed shipments of material and items.
Poor Shipment and Delivery Accuracy	Shipment accuracy implies that items are properly fulfilled, packed, and delivered in accordance with the customer's requirements.
Poor Delivery Performance	Poor delivery performance includes incorrect and incomplete shipments, shipments to the wrong location, and late shipments.
Loss of Cargo	Cargo loss means any loss or destruction that occurs while the cargo is moved within distribution channels.
Changes in Trade Policy (containers in ports)	See Office of the U.S. Trade Representative (https://ustr.gov/)
Accidents	An incident that happens unexpectedly and unintentionally, typically resulting in damage, injury, and negatively impacts the transportation network.

