Space Information Sharing and Analysis Center

Terms of Reference

v1.0. July 2020

(This Page Intentionally Blank)

Table of Contents

1. Purpose

The following acronyms and terms are provided as initial terms of reference. They were initially approved by the S-ISAC ISWG in Spring, 2020 as part of the vendor selection process when these terms were included with the vendor Request for Information. These will eventually be published elsewhere for ease of reference and maintenance.

Acronyms

API	Application Programming Interface
ASN	Autonomous System Number
CIDR	Classless Inter-Domain Routing
CISA	Cybersecurity and Infrastructure Security Agency
CMMC	Cybersecurity Maturity Model Certification
CMMI	Capability Maturity Model Integration
CONOPS	Concept of Operations
CSV	Comma Separated Values
EDA	Exploratory Data Analysis
EDR	Endpoint Detection and Response
FEDRAMP	Federal Risk and Authorization Management Program
FIPS 140-2	Federal Information Processing Standard Publication 140-2
GUI	Graphical User Interface
IAM	Identity and Access Management
IOC	Indicator of Compromise
ISAC	Information Sharing and Analysis Center
JSON	JavaScript Object Notation
MBC	Space ISAC Membership and Benefits Committee
Mutex	Mutual Exclusion Object
NIST	National Institute of Standards and Technology
NIST	National Institute of Standards and Technology
NUDET	Nuclear Detonation
PIR	Priority Intelligence Requirement
SIEM	Security Information and Event Management
SLA	Service-Level-Agreement
SP	Special Publication
STIX	Structured Threat Information Expression
TAXII	Trusted Automated Exchange of Indicator Information
TIP	Threat Intelligence Platform
TLP	Traffic Light Protocol
TLP	Traffic Light Protocol
TTP	Tactics, Techniques and Procedures
TTPs	Tactics, Techniques and Procedures
US-CERT	United States Computer Emergency Readiness Team

Terms

Term	Definition
Actionable Intelligence	Transformative information as a timely and relevant answer to leadership requirements, giving enough recommendation or course of action to enhance decision making.

Acumen	The ability to make good judgments and quick decisions, typically in a particular domain.
Alternate Board Member	Attends Board of Directors meetings with power to vote on behalf of Member in the absence of the Board Member.
Authorized User	An employee or affiliate in good standing of a Member who has been sanctioned by the Primary Contact of Member to have access to the ISAC Portal.
Board Member	The Individual who is designated by the Member organization to serve as the primary representative of Member on the S-ISAC Board of Directors.
CC (Common Criteria)	Common Criteria for Information Technology Security Evaluation (CC). Products can be evaluated by competent and independent licensed laboratories so as to determine the fulfilment of particular security properties, to a certain extent or assurance.
Center of Gravity (Cyber Frameworks)	Primary source that possesses the inherent capability to achieve the objective.
CMMC (Cybersecurity Maturity Model Certification)	CMMC is a vehicle the US Government is using to implement a tiered approach to audit contractor compliance with NIST SP 800-171 "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations."
CMMI (Capability Maturity Model Integration)	CMMI models have expanded beyond software engineering to help any organization in any industry build, improve, and measure their capabilities and improve performance.
Common Body of Knowledge	a core framework of all the relevant subjects a practitioner should be familiar with. A set of concepts, terms and activities that make up a professional practice, mastery over which is required for success in a field or profession.
Computed Indicators	"...those which are, well, computed. The most common amongst these indicators are hashes of malicious files, but can also include specific data in decoded custom C2 protocols, etc. Your more complicated IDS signatures may fall into this category." 45
C-Suite	A cluster of an organization's most important senior executives. C-suite gets its name from the titles of top senior staffers, which tend to start with the letter C, for "Chief," as in Chief Executive Officer (CEO).
Cyber Hygiene	Cybersecurity efforts are sometimes called "cyber hygiene." "Cyber hygiene includes such activities as inventorying hardware and software assets; configuring firewalls and other commercial products; scanning for vulnerabilities; patching systems; and monitoring." 46

Cyber Intelligence	Acquiring, processing, analyzing and disseminating information that identifies, tracks, and predicts threats, risks, and opportunities in the cyber domain to offer courses of action that enhance decision making.
Cyber Intelligence Framework	Analytical framework that provides a structure for cyber intelligence efforts. Components include; Environmental Context, Data Gathering, Threat Analysis, Strategic Analysis, Reporting and Feedback, and Human-Machine Teaming as a Center of Gravity.
Cyber Operations	Strategic employment of cyber capabilities where the primary purpose is to achieve objectives in or through the Cyber domain.
Cyber Threat Intelligence	Intelligence analysis on threats in the cyber domain. Cyber intelligence includes cyber threat intelligence, but cyber threat intelligence does not represent all of cyber intelligence. 48
Cyber Workforce	The total number of workers actively employed in, or available for work in the Cyber domain.
Cybersecurity	Actions or measures taken to ensure a state of inviolability of the confidentiality, integrity, and availability of data and computer systems from hostile acts or influences. 47
Data Gathering	Through automated and labor-intensive means, data and information is collected from multiple internal and external sources for analysts to analyze to answer organizational intelligence requirements.
Data Loss Prevention (DLP) Tool/Software	"Detects potential data breaches/data ex-filtration transmissions and prevents them by monitoring, detecting and blocking sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage)." 49
Data Source Validation	Checking the accuracy and quality of source data before using, importing or otherwise processing data.
Decision Support	An information system that supports business or organizational decision-making activities.
Diamond Model of Intrusion Analysis	"model establishing the basic atomic element of any intrusion activity, the event, composed of four core features: adversary, infrastructure, capability, and victim. These features are edge-connected representing their underlying relationships and arranged in the shape of a diamond, giving the model its name: the Diamond Model." 50
Discipline	A branch of knowledge. Disciplines may include Security, Intelligence, Forensics, Engineering, Data Science, or Knowledge Management to name a few.
Domain	A specified sphere of activity or knowledge. Domains are where humans interact. The physical domains of Air, Sea, Land, Space are now joined by the logical domain of Cyber.

Environmental Context	Everything you need to know about your organization internally and externally. Includes understanding organization's entire attack surface; and threats, risks and opportunities targeting your organization and industry, and the impact of those threats, risks and opportunities to your organization and industry. Includes deeply knowing your internal and external network and operations, to include but not limited to: the organizations servers, operating systems, endpoints, data centers, organization's business, its mission and culture, organizational processes and policies, business partners, geopolitics, emerging technologies, and position in industry relative to competitors. Attaining Environmental Context is a continuous process and influences what data is needed to perform cyber intelligence.
Estimative Language	Terms used in analytic reporting to convey the likelihood and impact of events or incidents.
FedRAMP (Federal Risk and Authorization Management Program)	The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Per an OMB memorandum, any cloud services that hold federal data must be FedRAMP authorized.
FIPS (Federal Information Processing Standards)	National Institute of Standards and Technology (NIST) develops FIPS publications when required by statute and/or there are compelling federal government requirements for cybersecurity.
Founding Member	A Member that joined as one of the Founding Members and thereby has a voting seat on the S-ISAC Board of Directors.
Human-Centered Design	"Design and management framework that develops solutions to problems by involving the human perspective in all steps of the problem-solving process. Human involvement typically takes place in observing the problem within context, brainstorming, conceptualizing, developing, and implementing the solution." 51
Impact	"Measure of effect or influence of an action, person, or thing on another—extended definition: may occur as either direct or indirect results of an action." 52
Indicator	Information that suggests an attack is imminent or is currently underway or that a compromise may have already occurred. Indicators can be used to detect and defend against potential threats. Examples of indicators include the Internet Protocol (IP) address of a suspected command and control server, a suspicious Domain Name System (DNS) domain name, a Uniform Resource Locator (URL) that references malicious content, a file hash for a malicious executable, or the subject line text of a malicious email message.

Information Requirements	Often used interchangeably with intelligence requirements. See intelligence requirements.
Information Sharing	Facts conveyed to maintain the confidentiality, integrity and availability of data.
Intelligence	"1. The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. 2. The activities that result in the product. 3. The organizations engaged in such activities." 53
Intelligence Requirements	An executive leadership requirement for intelligence to fill a gap in knowledge used in decision-making. The most important intelligence requirements to the organization will be deemed at executive level to be Priority Intelligence Requirements (PIR). See PIR.
Intelligence Sharing	Acquiring, processing, analyzing, and disseminating information that identifies, tracks, and predicts threats, risks, and opportunities in the cyber domain to offer courses of action that enhance decision making.
Intent	"Determination to achieve an objective." 54
Likelihood	"Chance of something happening, whether defined, measured or estimated objectively or subjectively, or in terms of general descriptors (such as rare, unlikely, likely, almost certain), frequencies, or probabilities." 55
Lockheed Martin Kill Chain	"The Cyber Kill Chain framework is part of the Intelligence Driven Defense model for the identification and prevention of cyber intrusions activity. The model identifies what the adversaries must complete in order to achieve their objective." 56
Machine Learning	A field at the intersection of Statistics & Computer Science. Fundamentally, it is about learning from data: summarizing patterns, making predictions, and identifying key characteristics of a group of interest, among many other tasks.
Member	An entity (company or a non-profit organization) that has been invited and agreed to join S-ISAC and is up-to-date with Membership dues.
MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)	"A globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community." 57

Office of the Director of National Intelligence, Cyber Threat Framework	"Developed by the US Government to enable consistent characterization and categorization of cyber threat events, and to identify trends or changes in the activities of cyber adversaries. The Cyber Threat Framework is applicable to anyone who works cyber-related activities, its principle benefit being that it provides a common language for describing and communicating information about cyber threat activity. The framework and its associated lexicon provide a means for consistently describing cyber threat activity in a manner that enables efficient information sharing and cyber Threat Analysis, that is useful to both senior policy/decision makers and detail oriented cyber technicians alike." 58
Operational Analysis	Analysis of specific threats, threat actors, their campaigns, intentions and capabilities against an organization and its industry. Operational Analysis answers Priority and specific intelligence requirements (PIR, SIR) to enhance CSO/CISO and other mid-to senior-level decisionmakers' leadership decisions regarding non-immediate but near-term (weekly–quarterly) business process and cybersecurity decisions.
Operational Environment	The combination of conditions, circumstances, and influences which will determine the use of resources and help executive leaders make decisions.
Organizational Impact	Generally maps to the U.S. DHS definition of Impact.
Organizational Intelligence Priorities Framework (OIPF)	A framework for creating and managing organizational intelligence requirements (IRs, PIRs, and SIRS) , the data sources aligned to answer those intelligence requirements, and the validation of those data sources. The OIPF informs future planning, budgeting, programming, and allocation of resources to data collection and analysis.
Participant	An authorized representative of a Member who participates in a limited-attendance meeting or conference or with a subcommittee. In some cases, for example if TLP Red information is shared in a meeting or a conference or with a subcommittee, the information can only be shared among fellow physical participants in that activity.
Practitioner	A person actively engaged in an art, discipline, or profession, especially in the Cyber domain.
Predictive Analysis	Encompassing a variety of techniques from data mining, predictive modelling, and machine learning, to analyze current and historical facts and make predictions about future or otherwise unknown events and incidents.
Primary Contact	An employee or affiliate in good standing of a Member who has been designated by Member to represent the Member and ensure that Members employees, agents and consultants who use S-ISAC will comply with this Operation and Analysis Framework.

Priority Intelligence Requirements (PIR)	Those intelligence requirements at the executive level that are most critical to the overall organization. These summarize the most important threats to the organization. Also called PIR. Answered by analysis of one or more specific information requirements (SIR)
Reporting and Feedback	Communication between analysts and decision makers, peers, and other intelligence consumers regarding their products and work performance. Reporting and feedback help identify intelligence requirements and intelligence gaps.
Return on Investment (ROI)	Performance measure used to evaluate the efficiency of an investment.
Risk	"Potential for an unwanted outcome as determined by its likelihood and the consequences...potential for an adverse outcome assessed as a function of hazard/threats, assets and their vulnerabilities, and consequences." 59 Exposure to consequence (loss); calculated as 'Likelihood times Impact' of an incident or event triggered by a threat. Risk technical and non-technical examples include Regulatory and Compliance, Privacy, Fraud, Geopolitical (Country-Nexus) and Cyber Attack.
Risk Assessment	Determination of the likelihood and impact of events and incidents resulting in positive or negative consequence and organization tolerances. Risk assessment is an inherent part of a broader risk management strategy to "introduce technical and non-technical control measures to eliminate or reduce" any potential negative risk-related consequences.
Risk Management	Risks can generally be managed four ways: avoided (i.e.: prevent from occurring), mitigated (i.e.: actions in advance to minimize damage if it occurs), transferred (i.e.: insurance) or accepted.
Security Operations	Discipline specific operations that deal with security issues on an organizational and technical level.
Security Orchestration, Automation and Response (SOAR)	"Technologies that enable organizations to collect security data and alerts from different sources." 60
SP (NIST Special Publications)	NIST Special Publications. Guidelines, technical specifications, recommendations and reference materials, comprising multiple sub-series: - SP 800. Computer security. SP 800 publications are developed to address and support the security and privacy needs of U.S. Federal Government information and information systems. - SP 1800. Cybersecurity practice guides. - SP 500. Information technology (relevant documents).

Specific Intelligence (or Information) Requirements (SIRs)	Observables; can be collected/observed in the physical or virtual world. These requirements once analyzed may provide answers to one or more priority intelligence requirements (PIR).
Strategic Analysis	The collection, processing, analysis, and dissemination of intelligence that is required for forming policy and plans at the 'C-Suite' and Board level. Strategic Analysis is the process of conducting holistic analysis on threats AND opportunities. Holistically assessing threats is based on analysis of threat actor potential, organizational exposure and organizational impact of the threat. One might also perform Strategic Analysis to provide deep clarity on the who and why behind threats and threat actors. Strategic Analysis goes beyond Threat Analysis to incorporate analysis regarding emerging technologies and geopolitics that may impact/provide opportunities for the organization now and in the future. In this light, Strategic Analysis is not only comprehensive, but ANTICIPATORY. It can be actionable, yet is based more on analytical judgments, enabling executive leaders to make risk-based decisions pertaining to organizational wide financial health, brand, stature, and reputation.
Structured Analytical Techniques	Analytic techniques designed to help individual analysts challenge their analytical arguments and mind-sets. Techniques are grouped by diagnostic, contrarian and imaginative thinking.61
Tactical Analysis	Analysis of specific threats, attacks, incidents, vulnerabilities, or unusual network activity that enhances decision making for network defenders, incident responders, and machines pertaining to cybersecurity and incident response. Information analyzed is usually technical telemetry such as network and endpoint activity, atomic, behavioral, and computed indicators62 such as: malware samples, hash values, domains, IPs, logs, email header information. Tactical analysis tends to answer specific intelligence requirements (SIRs) and the immediate, daily and weekly what/where/when/how questions about threats.
Target Exposure	Generally maps to the U.S. DHS definition of Risk.
Threat	Trigger to consequence (loss); resulting from a person, group, or thing with capability and intent to inflict consequence. Threat technical and non-technical examples include autonomous Artificial Intelligence, Advanced Persistent Threats (APTs), Insiders, Nature, etc. “Indication of potential harm to life, information, operations, the environment and/or property—extended definition—may be a natural or human-created occurrence and includes capabilities, intentions, and attack methods of adversaries used to exploit circumstances or occurrences with the intent to cause harm.” 63

THREAT (Formula)	RISK + LIKELIHOOD + IMPACT. Some definitions also weight the threat by using impact as a multiplier (calculate as RISK + LIKELIHOOD TIMES impact...vice plus impact).
Threat Analysis	Assessing technical telemetry and non-technical data pertaining to specific threats to your organization and industry to inform cybersecurity operations/actions and Strategic Analysis. Threat Analysis is built on operational and tactical analysis and enhances CSO/CISO and other mid- to senior-level decision making.
Threat Information	Any information related to a threat that might help an organization protect itself against a threat or detect the activities of a threat actor.
Threat Intelligence	Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision making processes.
Tradecraft (Cyber Intelligence)	Tools, techniques, and procedures used to acquire, process, analyze, and disseminate information that identifies, tracks, and predicts threats, risks, and opportunities in the cyber domain to offer courses of action that enhance decision making.
Vulnerability	Path to consequence (loss); as an avenue of access, control, or influence that can inflict consequence. Vulnerability technical and non-technical examples include unpatched systems, poor coding practices, employees with no cybersecurity awareness, etc.
Sources	41 https://ai.cs.cmu.edu/about 42 https://digital-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain 43 https://digital-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain 44 https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHS-Lexicon.pdf 45 https://digital-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain 46 https://www.nist.gov/blogs/taking-measure/rethinking-cybersecurity-inside-out Ron Ross. November 15, 2016

47 The definition for cybersecurity created based on analyzing participating organizational responses and from the DHS Lexicon Terms and Definitions Instruction Manual 262-12-001-01 (October 16, 2017) https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHS-Lexicon.pdf

48 A number of organizations expressed confusion over the difference between cyber threat intelligence and cyber intelligence, specifically whether these terms describe the same thing. Many organizations told us that introducing "threat" into this phrase breeds that confusion. Although threats are a large part of the cyber intelligence picture, cyber intelligence also includes analysis of areas like technologies, geopolitics, and opportunities. For these reasons, this report deliberately excludes the term "cyber threat intelligence." We refer to the activities typically associated with cyber threat intelligence as Threat Analysis, a component of the Cyber Intelligence Framework.

49 https://en.wikipedia.org/wiki/Data_loss_prevention_software

50 https://apps.dtic.mil/docs/citations/ADA586960

51 https://en.wikipedia.org/wiki/Human-centered_design

52 DHS Lexicon Terms and Definitions Instruction Manual 262-12-001-01 (October 16, 2017) https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHSLexicon.pdf

53 https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf

54 DHS Lexicon Terms and Definitions Instruction Manual 262-12-001-01 (October 16, 2017) https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHSLexicon.pdf

55 https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHS-Lexicon.pdf

56 https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

	57 https://attack.mitre.org 58 https://www.dni.gov/index.php/cyber-threat-framework 59 DHS Lexicon Terms and Definitions Instruction Manual 262-12-001-01 (October 16, 2017) 60 https://www.gartner.com/en/documents/3860563 61 https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf 62 https://digital-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain 63 DHS Lexicon Terms and Definitions Instruction Manual 262-12-001-01 (October 16, 2017) https://www.dhs.gov/sites/default/files/publications/18_0116_MGMT_DHSLexicon.pdf

(This Page Intentionally Blank)