Cyber Semantic Landscape Ontology and Taxonomy

The Cyber Semantic Landscape Ontology and Taxonomy (CSLOT) provides a structured approach to the dynamic needs of the Cyber security concepts, theories, standards, and compliance issues facing the 21st century of consumers. The CSLOT provides this by deconstructing associated activities into logical processing objects to provide the highest level of pre-analysis required to develop a discrete understanding for a given Cyber engagement to include technical and non-technical personnel within the Cyber Workforce. The construction of the CSLOT requires both a semantic and taxonomy fusion capability to provide the required analysis steps and processes to achieve the desired outcome of Cyber excellence. The ability to organize the specific activities of a given outcome requires that each be defined, structured and implemented with a measured outcome or vetting activity to deliver the evidence of proof. The approach defined within the CSLOT incorporates eight specific activities to provide a repeatable orientation perspective to the development identifying risks, standards, and provide a means, method and capability that are required to operate within a Cyber environment.

Any organization has a strong commitment to the protection of is corporate identity, brand and intellectual property. The CSLOT provides an insight into our level of organization theory, thought, leadership and practical standards of implementation in establishing Cyber excellence. The CSLOT provides an organizational approach to manage our commitment to our shareholders, clients, stakeholders, and employees on the importance of Cyber Awareness and Resilience (CAR), a primary tenant of our dynamic security approach. We understand the importance of CAR and have defined our processes and offerings around a strategic commitment to Cyber excellence. We understand the importance of providing the most qualified workforce, which includes the ability to train to understand the Cyber Security Decision Matrix (CSDM) and delineated within the Cybersecurity Workforce Framework (NCWF) and its alignment with all known federal, state and local standards to ensure that our evidence based approach provides the required measure of known good to all parties involved.

The CSLOT has eight levels, which are provided below with descriptions of services for an approach to Cyber excellence. Each level should be completed in its entirety prior to proceeding to the next level and each should have a training element associated with the knowledge requirements, job description and common task functions required for each level. A general description is provided below for an evidence approach to how the organization approaches the responsibility of CAR and Cyber Excellence.

Level 1: Domain Awareness – provides for organizational awareness on how to conduct Cyber Situational required activities.

Information Technology Cyber Conflict Divergence (ITCCD) – provides a Cyber orientation of primary and specialized knowledge levels of a given activity. The need to understand how each Cyber concept affects the landscape begins by defining who has what operational knowledge of the given task, problem or operation to determine the ability to measure the Cyber cognizance contribution into the dynamic leadership management paradigm. The two areas of primary and specialized knowledge are further broken down to provide conceptual decision-making responsibilities and accountability activities.

Joint Architecture Reference Model (JARM) – provides the Department of Defense (DoD) approach to how both Cyber and Operational concepts would provide for cross-supporting activities and engagement. The ITCCD and JARM can be blended together to provide the required security posture required for DoD clients.

Level 2: Cyber Risk Compliance and Information Assurance (CRCIA) – Provides a centralized method to identify all known risks, compliance, information assurance and applicable frameworks to achieve a viable security posture. The CRCIA, incorporates the Cyber Security Framework (CSF), Risk Management Framework (RMF), Continuous Monitoring Framework (CMF), NICE Cybersecurity Workforce Framework (NCWF), Cyber Resiliency Engineering Framework (CREF), Supply Chain Risk Management Framework (SCRMF), Policy Awareness Framework (PAF), Forensic Investigation Framework (FIF) into a unified analysis model to define, process and describe the organizational security Cyber risk posture for clients.

Level 3: Cyber Order of Operations and Methodology (COoOM) – provides a method for building the required security control baseline, that transcends human bias in security control selection to include analysis of the many varied states of a given security control. Additionally, the Federal Information System (FIS) and Non-Federal Information Systems (NFIS) analysis required for the different versions of the NIST SP 800-53 are defined to build a comprehensive security control baseline, which provides the highest level of security analysis required to achieve a known Cyber Risk posture for our clients.

Level 4: Common Cyber Threat Framework (CCTF) – provides a common means and method of how to standardize the language of Cyber related activities and enables a consistent categorization of a threat. The four layers are 1) Stages, 2) Objectives, 3) Actions and 4) Indicators. The CCTF has several sub-processes, which enables the framework to define capabilities of defined targets and measure the outcomes of the attack profile. Each layer of analysis requires a defined prosecution of a given Cyber threat to determine likelihood and the outcome of the process would define the validity of a Cyber-attack vector for analysis by Level 5

of the model. This provides a simple, yet flexible, collaborative way of characterizing cyber activities that supports analysis for all levels of Cybersecurity.

Level 5: Cyber Vulnerability Reporting Framework (CRVF) – provides a data fusion analysis capability to look at the landscape of Vulnerabilities into a single ontology and taxonomy to define the data structure for storing and conducting analysis for the validation of a Cyber threat to determine likelihood of effect or consequence on an Information Systems that has been defined as mission critical. The CRVF leverages the Common Vulnerability and Exposure (CVE), National Vulnerability Database (NVD) and Vulnerability analysis provided by the National Institute of Standards and Technology (NIST) and the National Vulnerability Database (NVD) managed by the US CERT program to provide a unified analysis capability to determine the attack vector and common mitigation processes to resolve a known security issue.

> The CVE, NVD and Vulnerabilities provide a unified framework for reporting, researching and conducting analysis of past, present and emerging Cyber Vulnerabilities to achieve a dynamic means and method to determine analysis requirements for any information system. The ability to search each system dynamically offers the outcome of fusion analysis using common lexicon mapping to known security controls provided by the NIST SP 800-53 and keyword associated activities. Additionally, the collection of the history of a given security vulnerability provides richness for contextual analysis required for Cyber Awareness and Resilience (CAR), a primary tenant of the CSLOT approach. This provides a measurement of a risk profile based on the likelihood of attack assigned to a known vector of attack.

Level 6: Cyber Artifact Repository Framework (CARF) – A common repository of Cyber related artifacts required to demonstrate the current, past and future continuous monitoring requirements for a given system. Common artifacts would include the following; however, could be expanded to demonstrate totalitarian documentation for a given system or systems: 1) Security Control Baseline (SCB), 2) System Security Plan (SSP), 3) Plan of Action and Milestone (POA&M), 4) Legal, 5) Risk Management Framework Profile (RMFP), and 6) Security Content Automation Protocol (SCAP).

Level 7: Cyber Resiliency Review (CRR) – Provides a prescriptive analysis phase that defines the various elements of CAR with assessment for evidence and validation of reporting security standards to determine the maturity indication level (MIL) for a given information system. The CRR has 12 elements that work together to provide a binary analysis of the organizational information systems, which include: 1) Asset Management, 2) Controls

Management, 3) Configuration and Change Management, 4) Vulnerability, 5) Incident Management, 6) Service Continuity Management, 7) Risk Management, 8) External Dependencies Management, 9) Training and Awareness, 10) Situational Awareness, 11) Goals and Questions, and 12) Maturity Indicator Level (MIL). The MIL has five levels, each of which defines the level of evidence provided by the organization to demonstrate the adherence to the described standards for CAR and CRR overview analysis can provide a measurement to provide a Risk Assessment Posture (RAP) score for Clients.

Level 8: Deep Analysis – The ability to blend the concepts of Artificial Intelligence (AI), Natural Language Processing (NLP) and Deep Package Analysis required the unification of various research disciplines into a common approach lexicon for Cybersecurity operationalization. The Cyber Predictive Helix Analysis Capability (CPHAC) solution provides the ability to describe Cyber relationships and document the potential impacts from several discrete perspectives to develop a derived security analysis. The CPHAC provides the backbone for analysis by building the required dynamic relationship and includes the organization structure analysis required to execute an organizational approach to CAR and the preceding seven levels of the CSLOT. Each of the eight layers work in unison to provide for the highest degree of measured Cyber adherence and is the common lexicon for the organizational approach to internal best practices and the services offered to our clients.

The CPHAC is our premier as a service offering, which we use to help define, organize and discover the various Cyber related activities to determine our unified approach to security. The CPHAC provides means, methods and capability for documenting dynamic and discrete relationships found in the Cyber domain. It incorporates the ability to find hidden relationships between vendor products and security controls. The organizational structure provides a visualization of the required concepts needed to engage on any cyber activity to bring about the highest level of CAR and Cyber excellence possible because of its defined method for security concepts mapping and use of dynamic risk calculations for a myriad of uses. Distinct analysis provides insight into fusion analysis, which then provides more analytic analysis requirements to discover the various states of CAR within a given CSLOT or specific level of CSLOT.

For example, the ability to align the impact for the OMB Circular A-130 to the NIST SP 800-53r5, including the documentation of the 18 different states of a given security control, and the roles and responsibilities for evidence and forensic analysis standards to ensure that any organization achieves the CAR goals and has the added ability to define the Cyber Security Framework (CSF) elements that reinforce the needs for the US CERT Cyber Resilience Review (CRR) tenants to provide the evidence to prove that we do what we say we are doing. All

organizations should strive to achieve a “baked in security” approach that is the true standard by which all organizations should be measured by and we invested in the CPHAC to help make that our concentric circles of cyber edge offerings to provide the highest level of security. Our approach required taking a forensic analysis phase and overlay with a criminal investigation phase and blend the outcome together to achieve our end state of CAR and Cyber excellence.

For Additional Information Contact:

Eigenspace
312 Main Street, Suite 300
Gaithersburg, MD 20878
240-654-4097
www.eigenspace.us