

Cybersecurity Order of Operations Methodology

The draft release of the NIST SP 800-53 Rev. 5, scheduled for December 29, 2017 and its potential impact, the need to develop a method that provides a preemptive analysis capability will be required to achieve the guidance outlined by the document. Currently, Eigenspace is proposing two US Federal organization and commercial organization that deal with privacy impacting data sets and non-privacy impacting data sets. The Controlled Unclassified Information (CUI) impacts, of the NIST SP 800-53r5 are still under assessment.

Tetradecagon - is a 14-side polygon and has various elements associated with how to approach building a new security control baseline as outlined in the document; however, knowing where to start the process is almost as important as the outcome. Hendecagon - is an eleven-sided polygon has similar elements minus the privacy impacts. The two methods are collectively labelled as the Cyber Security Order of Operations (CSOoO) as a concept. In the commercial world you have a non-privacy and privacy elements, which are respectfully called Quadrilaterals and Hexagon. Quadrilaterals - is a four-sided polygon with privacy impact analysis requirements. Hexagon - is a six-sided polygon with privacy impact analysis requirements.

The Cyber Multi-Sided Analysis and the Cyber Order of Operations

The proposed draft of the NIST SP 800-53 Rev. 5 creates onto itself a degree of complexity, dexterity and acumen that has been missing in the modern Cyberspace landscape. NIST was given an impossible task to make a 180-degree turn on a dime and produce a result that would begin to immediately increase the definition of known good for the entire federal government and those that support them in the mission activities required. The effort that it took to achieve this objective begins with understanding the Office of Management and Budget (OMB) needs, such as the OMB Circular A-123, Circular A-130, M 17-05 and M 17-25, thanks to Aaron Bishop for his contribution on this emerging topic of discussion. Let's consider for a moment that next withdrew 127 security controls and replace them with an additional 50 security controls, removed Confidentiality, Integrity, Availability and replaced them with almost 14-states that a control could or might have within any given system or systems, and our organization; and various owners of the that control.

The resulting control types, the embedding of privacy and assurance within the control statement and supplemental guidance. The increase of related security controls aligned with a keyword index search capability that includes thematic themes, concepts, ideas and the documentation of industry best practices all aligned to security controls. In short, the single most

Cybersecurity Order of Operations Methodology

comprehensive NIST SP 800-53 known with true Cybersecurity rules, responsibilities and accountability for a lack of leadership and vision. The ability to defer, select your own version of Cybersecurity depends on whom you are supporting and how, when, where and which controls might be violated place a legal aspect not before seen in previous versions.

Cyber Order of Operations Methods (COoOM)

As stated above, the Tetrdecagon - is a 14-side polygon and has various elements associated with how to approach building a new security control baseline as outlined in the document; however, knowing where to start the process is almost as important as the outcome. This concept posited in a previous article was made real with the aid of a significant contribution already mention in this article, Mr. Bishop whom decided to push the point of theory and ask for an approach, means, method or activity that would be required to determine the significance of the new guidelines from as many perspectives as possible. The results are nothing short of alarming in the Cyberspace, not so much, but for others a complete disbelief and instant pandering that what has been written, is not true and unachievable.

The tetrdecagon requires a complexity understanding of some simple decision points and an order of decision-making that is much like a choose your own adventure reading book from the early 80's. The intent of this article is to demonstrate the level of pre-analysis required to achieve a semblance of a repeatable process with an embedded outcome process based on the response and needs of the individual, organization, program or service.

The first part of the tetrdecagon is the selection of the 912 potentially active security controls, which we will call the Angle Active (AA) or $AA = 912$.

The second part of the tetrdecagon is the sub-selection of the 52 potential required security controls, which are represented as Angle Required (AR) or $AR = 52$.

The third part of the tetrdecagon is the sub-selection of the 92 OMB Circular A-130 potential security controls, which are represented as Angle OMB Circular A-130 (AO) or $AR = 92$.

The fourth part of the tetrdecagon is the sub-selection of the 234 Cyber Security Framework potential security controls, which are represented as an Angle Cyber Security Framework (ACSF) or $ACSF = 234$.

Cybersecurity Order of Operations Methodology

The fifth part of the tetradecagon is the sub-selection of the 115 Cyber Security Framework Identity potential security controls, which are represented as Angle Cyber Security Framework Identity (SACSFI) or ACSFI = 115.

The sixth part of the tetradecagon is the sub-selection of the 239 Cyber Security Framework Protect potential security controls, which are represented as Sub-Angle Cyber Security Framework Protect (SACSFP) or ACSFP = 239.

The seventh part of the tetradecagon is the sub-selection of the 81 Cyber Security Framework Detect potential security controls, which are represented as Sub-Angle Cyber Security Framework Detect (SACSFD) or ACSFD = 81.

The eighth part of the tetradecagon is the sub-selection of the 49 Cyber Security Framework Respond potential security controls, which are represented as Sub-Angle Cyber Security Framework Respond (SACSFR) or ACSFR = 49.

The ninth part of the tetradecagon is the sub-selection of the 11 Cyber Security Framework Recover potential security controls, which are represented as Sub-Angle Cyber Security Framework Recover (SACSFR_e) or ACSFR_e = 11.

The tenth part of the tetradecagon is the sub-selection of the 158 Privacy potential security controls, which are represented as the Angle Privacy (AP) or AP = 158.

This step may have three or more independent steps that are as follows:

- a. Privacy Act of 197
- b. Health Insurance Portability and Accountability Act (HIPPA) of 1996
- c. Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009

The eleventh part of the tetradecagon is the sub-selection of the 344 Assurance potential security controls, which are represented as an Angle Assurance (AAS) or AAS = 344.

The twelfth part of the tetradecagon is the inclusion of the FISMA potential security controls, which are represented as Angle FISMA (AFISMA) or AFISMA = 18.



Cybersecurity Order of Operations Methodology

The thirteenth part of the tetradecagon is the analysis of the FISMA selected security controls, which are represented as the proposed baselines and has numerous analysis points and decision approaches, which are as follows:

Control Type Analysis

Common, System-Specific, Hybrid, Joint, Situational Required,
Discretionary, Withdrawn

Conversion Process: Confidentiality, Integrity, Availability

Implementation Type: S, O, O/S

Baseline: Unassigned, Low, Moderate, and High

The fourteenth part of the tetradecagon is the sub-selection of the 279 Department of Justice (DoJ), Federal Bureau of Investigations (FBI), Criminal Justice Investigation Services (CJIS) potential security controls, which are represented as Angle Legal (AL) or AL = 279.

Thus, each organization should consider building a Cyber Order of Operations Method (COoOM) to achieve their desired security posture. Thanks to Mr. Bishop for providing an excellent argument point stay tuned as Eigenspace continues to research into finding logic, reason, method, and analysis of this change for the United States and all sub-contracting organizations that support them.

For Additional Information Contact:

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