# An Investigation of Data Sharing for DoD DCO Forces


## Sienne Rodwell

### CyberSecurity Service Provider Internship Program, ICS 296 & 396, Spring 2023

### Advisors: Dr. Curtis Arnold, Chief Scientist – Cyber, & Dr. Robert Adamove, Sr. Associate, (Core4ce)


## Problem Statement:

The problem is that the DoD has yet to create a standard for data sharing across DCO forces (Castillo, 2020). Modern cybercriminals are becoming increasingly difficult to combat on account of improved techniques, tactics, and procedures (TTPs), as well as increased persistence, motivation and funding (Abu et al, 2018). To effectively combat these criminal forces, data such as log entries, alerts, and reports must be shared across cybersecurity organizations (Katos et al, 2020). Despite the understood benefits and necessity, successful cybersecurity information sharing has been unachievable thus far (Simpson et al, 2019).

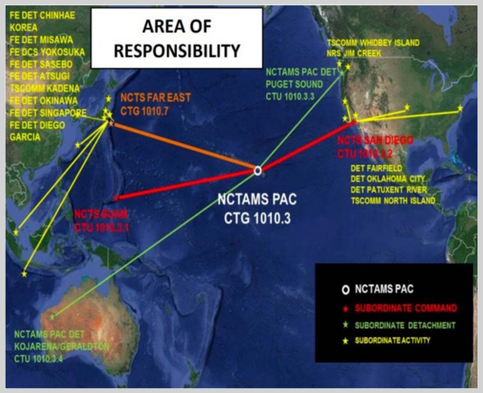
## Purpose:

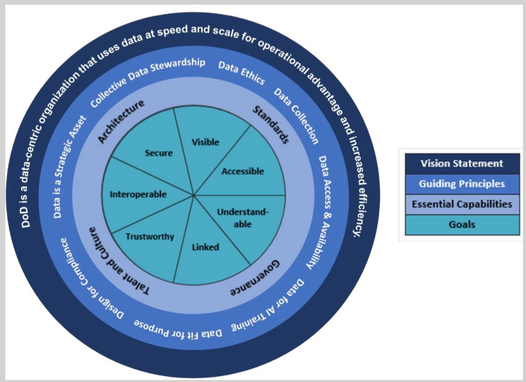
The purpose of this study is to evaluate the status of DoD DCO data sharing and identify what is needed to improve data sharing across DCO forces. The goal of the DoD is to create a data-sharing environment and culture in which data is visible, accessible, understandable, linked, trustworthy, and secure (DoD, 2020). This study serves as a consolidated information base for issues as well as possible solutions for cyber threat information sharing following the DoD's intent,. This study contributes to current scholarship by providing a summary of DoD intent, current issues, and perceived barriers, as well as an analysis of some of the currently proposed solutions. It is intended that this study be used to inform he reader of the status of cyber threat information sharing regarding both the issues experiences ubiquitously across cyber defense fields as well as solutions that could be implemented or expanded upon to contribute to defense against increasing cyber attacks.

## Approach:

To attain the content of this study, a literature review and interviews were conducted. To attain academic literature, the University of Hawaii (UH) at Manoa and Google Scholar Databases were the primary search mechanisms. Using these databases, many sources such as the Institute of Electronical and Electronics Engineers (IEEE) explore, Association for Computing Machinery (ACM) conferences, DoD executive summaries, and a range of postgraduate studies were incorporated. Keywords and phrases used in the acquisition of these sources include "DoD data sharing", "big data security", "data sharing", "DoD data sharing DCO forces", and "cybersecurity information sharing".

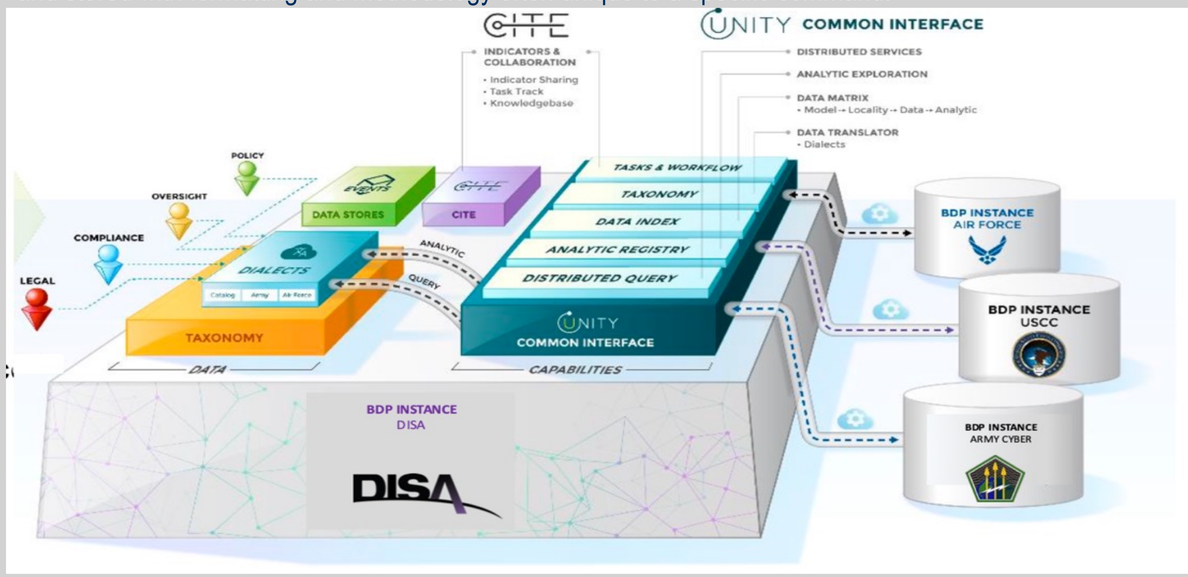
Through the above, a great number of issues as well as possible solutions were revealed. This study evaluated the intent and goals of the DoD, the status of tools used and information sharing, current issues, perceived barriers for information sharing, and multiple proposed solutions.




## Discussion & Conclusion:

It was found that the DoD is in the process of a culture shift from "need to know" to "responsibility to provide" for data sharing. In doing so, many issues have arisen, especially regarding DCO forces. This study found that interoperability is among the most considerably challenges faced by intelligence commands. While there are some tools which are commonly used, many commands use differing tools, causing data to be both presented and stored with formatting and methodology often unique to a specific command.




With some exceptions, it is accepted that data sharing is a vital part of DCO forces in both government and private sectors. There have been many platforms created in the attempt to resolve the issue of data sharing on a large scale. This includes but is not limited to the CYBEX-P platform, blockchain based platforms such as iShare, and decision tree algorithm-based platforms. While these platforms may be effective solutions in some private organizations, due to the differences in need and environment of government cyber operations, they are unlikely to succeed in such a setting. The DoD is in the process of implementing a central data repository known as the Big Data Platform (BDP). DCO forces will be expected to provide data to this platform. Currently this process could prove to be quite disorganized and therefore largely unhelpful, as DCO forces create and store their data differently. A potential solution currently being developed is the use of a common information model (CIM). A CIM is not a data platform, but a standardized format for data transport. This would require minimal modifications to daily operations while still maintaining effective data sharing requirements. CIMs have already been successfully integrated in a large range of environments and can be manipulated to fit the specific needs of an organization.

## Path Forward:

The advancement and integration of a CIM or multiple CIMs is highly recommended. While there are many solutions available for private sector use, it is recommended that the DoD performs a "ground up" analysis of needs regarding DCO data sharing. Often in government organizations management and technical fields are highly separated, causing operations issues or ideas for improvement to go largely unnoticed by those with the power to act upon them.

## References:


Castillo, E. (2020). Information sharing within the FLTCYBERCOM/C10F organization. *Naval Postgraduate School*. https://apps.dtic.mil/sti/pdfs/AD1114632.pdf

DoD. (2020). Executive summary: DoD data strategy, unleashing data to advance the national defense strategy. *Department of Defense Office of Prepublication and Security Review*. https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF



INFORMATION & COMPUTER SCIENCES

UNIVERSITY *of* HAWAI'I *at* MĀNOA