Enterprise Security Configuration and Compliance (ESC2) System

# Description:

The US Department of Defense (DOD) creates Security Technical Implementation Guides (STIGs) for various types of technology. STIGs may cover implementing anything from operating systems (ubuntu, Windows, Mac, etc.) to applications (Chrome, Firefox, Adobe products, databases). A STIG provides steps to implement the technology it in a secure manner. Currently these guides are used only on government resources.

A new process is being developed called the Cybersecurity Maturity Model Certification (CMMC). Compliance with this specification will be required of all Federal contractors. It is intended to protect Controlled Unclassified Information (CUI) on these contractors’ electronic systems.

Examples of common categories of CUI

* Agriculture
* Critical Infrastructure
* Emergency Management
* Export Control
* Financial
* Geodetic Product Information
* Immigration
* Information Systems Vulnerability Information

The CMMC requirements are in a draft form currently, and the final format is uncertain. It is likely that Federal contractors are going to need to do more to secure their systems. There was a recent Colonial Pipeline hack that disrupted gasoline deliveries to the east coast in 2021. This incident is a prime example of how important it is that the electronic security be improved by Federal contractors and those supplying critical infrastructure and supplies.

It is likely that the final requirements from CMMC will be an extension upon the existing National Institute of Standards and Technology (NIST) document 800-171 which is titled "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations".

Section 3.4.2 in this document requires that companies "Establish and enforce security configuration settings for information technology products employed in organizational systems."

This statement is not specific as to what security configuration to apply. This forces companies to decide what is sufficient for each type of technology they utilize. This will be a significant task for each company to undertake. They may choose that is easier to just adopt the existing STIGs that the DOD has already defined.

The Enterprise Security Configuration and Compliance (ESC2) system will assist companies that are currently unfamiliar with STIGs to implement them and track them across their internal electronic systems.

# Desired System Outcomes

Companies using this system will be able to

* Track a list of technologies in use
* Track the company-controlled systems that implement these technologies
* Track the list of STIGs that cover the technologies
* View the requirements of each STIG
* View the status of security configuration of each company-controlled system
* Perform periodic audits of the company-controlled systems for compliance assurance
* Calculate the cost of security
* Track Log Activity

# Justification

This database system will assist customers in complying with future regulations that will be a part of future Federal contracts. Failure to comply with these regulations may result in the loss of contracts and their associated revenue.

# References

Bloomberg. (n.d.). Bloomberg.com. Retrieved October 30, 2021, from <https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password>.

Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., & Guissanie, G. (2021, January 28). *Protecting controlled unclassified information in nonfederal systems and organizations*. CSRC. Retrieved October 30, 2021, from https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final.

Armond, A. (2021, September 27). *Policy templates and tools for CMMC and 800-171*. CMMC Audit Preparation. Retrieved October 30, 2021, from https://www.cmmcaudit.org/policy-templates-and-tools-for-cmmc-and-800-171/.

Computer Security Division, I. T. L. (n.d.). *Protecting controlled unclassified information (CUI): CSRC*. CSRC. Retrieved October 30, 2021, from <https://csrc.nist.gov/Projects/protecting-controlled-unclassified-information>.

*NIST Computer Security Resource Center | CSRC*. (n.d.). Retrieved October 30, 2021, from https://csrc.nist.gov/CSRC/media/Publications/sp/800-171/rev-2/final/documents/CUI-SSP-Template-final.docx.

What are examples of controlled unclassified information? (n.d.). Retrieved October 30, 2021, from https://askinglot.com/what-are-examples-of-controlled-unclassified-information.

Sarah Knowlton, & Cyberx-Mw. (2021, October 28). *Security Technical Implementation Guides (STIGs)*. DoD Cyber Exchange. Retrieved October 30, 2021, from https://public.cyber.mil/stigs/.