Privacy Prerequisites

During the pre-internet days the control, monitoring, and accountability regarding sensitive federal, military, or corporate intellectual property was a tangible physical activity where hidden documents or other recognizable media could be uncovered simply by controlling people and physical facilities.

The majority of our federal and state laws were architected around physical property to preserve ownership and enable the owner to control privacy.

Pop culture explored those behaviors in numerous movies where nefarious state-actors would infiltrate a building to capture photographic images or out-right remove file folders and paper documents.

In this generation data as property was recognized and this historical method of control was the prerequisite for early digital information control processes.

Digital Era Privacy

The rapid on-set of information digitization and transmission mediums offer significant value in terms of search, access, exchange, and repository management yet created a version of information exchange much less understood thereby leaving business owners to deal with a much less tangible risk interpretation. Subsequently digitized information invokes a much lower human perception of value where users often leave files, server access, or user credentials in a dangerously exposed position.

The current implementation of the internet protocol and subsequent architecture of systems and software imposes a multifaceted attack surface upon digital infrastructure. No longer is it acceptable to simply guard office access sites or monitor employees, this is out of your control.

Third-Party Risk Factors

The United States government and corporations are under continuous cyber-attack from nation state actors, organized criminal groups and others who routinely seek to undermine and steal from federal, state and municipal governments, private and public companies and individuals. The Department of Defense (DoD) is a target of attack and nefarious actors understand that the DoD and Prime contractors have strong protections in place so they focus attacks across the supply chain on smaller more vulnerable companies.

These risks are further compounded through the growth in Software as a Service (SaaS) and Cloud service offerings. The data your company creates is now processed, inventoried, and exposed to a myriad of physical hardware systems, facilities, and third-party employees across many states and foreign jurisdictions. This model further disconnects data as property controls. There is additional data control risk incurred as many of these SaaS and Cloud services have foreign national ownership and employees.

Despite efforts of the DoD to improve cybersecurity hygiene across the supply chain with cooperation through the development and education of National Institute of Standards &

Technology (NIST) protocols such as NIST 800.171 there was no method to measure implementation and adherence. As of today, these have been primarily self-assessed and self-certify recommendations where in implementation has not achieved the desired results.

Cybersecurity Maturity Model Certification CMMC

The DoD has created the Cybersecurity Maturity Model Certification (CMMC) that applies to all organizations within the supply chain and enforces adherence across five levels of standards through audit by accredited compliance assessment organizations. The Department is implementing CMMC throughout fiscal year 2021 to 2025 phased rollout approach. Until September 30, 2025, the Office of the Under Secretary of Defense for Acquisition and Sustainment must approve the inclusion of the CMMC requirement in any solicitation. As of November 30, 2020, the DFAR 252.204-7012 Rule Change enabled the inclusion of CMMC on specific acquisitions. During this phased rollout Request for Proposals (RFPs) may include CMMC requirements of their contractors with flow-down to subcontractors.

While this effort, currently only applies to DoD supply chain contractors, these cybersecurity hygiene practices offer a good common-sense strategy for any corporation, association, or agency across any industry. All business owners will benefit as this protocol combines employee training, corporate processes, and IT equipment requirements relevant to your level of privacy requirements.

Compliance certification audits such as ISO are common practice in many industries where self-regulation is not effective and as such, we anticipate cybersecurity audits will also become commonplace. Similar to ISO qualification, Cybersecurity qualification will be a market advantage for the companies who publicly adhere to standards that protect the privacy of their customers and vendors while also ensuring business owner and shareholder value.

Enabling Corporate Compliance

Cybersecurity practices, IT system implementation and training will sound like an impossible task especially for the small and medium corporations with limited budget and workforce. Identifying and partnering with external parties will be critical in your success, protection, and certification.

When it comes to certification look to those DoD accredited service providers who know the CMMC protocol and more importantly how to interpret what is required for your particular type of business activities.

While dealing with the actual management of users, digital data, and auditability of your digital transactions between employee, customers, clients, and vendors Cicer One Technologies Inc offers a turn-key solution that is affordable and sustainable. The vast majority of subcontractor certification is estimated to be in the Level 1 to Level 3 range where the SCUTE product offers a simple compliance solution for any business. Cost effective and simple is critical especially for subcontractors where their DoD business may only be 10-40% of their total revenue.

SCUTE CMMC Compliance

CONTROLS	LEVEL 1	LEVEL 2	LEVEL 3
C001	AC.1.101	AC.2.005 AC.2.006	
C002	AC.1.002	AC.2.007 AC.2.008 AC.2.009 AC.2.010 AC.2.011	AC.3.012 AC.3.017 AC.3.018 AC.3.019 AC.3.020
C003		AC.2.013 AC.2.015	AC.3.014 AC.3.021
C004	AC.1.003 AC.1.004	AC.2.016	AC.3.022
C005			AM.3.036
C006			
C007		AU.2.041	AU.3.045 AU.3.046
C008		AU.2.042 AU.2.043	AU.3.048
C009			AU.3.049 AU.3.050
C010		AU.2.044	AU.3.051 AU.3.052
C011		AT.2.056	AT.3.058
C012		AT.2.057	
C013		CM.2.061 CM.2.062 CM.2.063	
C014		CM.2.064 CM.2.065 CM.2.066	CM.3.067 CM.3.068 CM.3.069
C015	IA.1.076 IA.1.077	IA.2.078 IA.2.079 IA.2.080 IA.2.081 IA.2.082	IA.3.083 IA.3.084 IA.3.085 IA.3.086
C016		IR.2.092	
C017		IR.2.093	
C018		IR.2.096	IR.3.098
C019		IR.2.097	
C020			IR.3.099
C021		MA.2.111 MA.2.112 MA.2.113 MA.2.114	MA.3.115 MA.3.116
C022			MP.3.112
C023		MP.2.119 MP.2.120 MP.2.121	MP.3.123
C024	MP.1.118		
C025			MP.3.124 MP.3.125
C026		PS.2.127	
C027		PS.2.128	
C028	PE.1.131 PE.1.132 PE.1.133 PE.1.134	PE.2.135	PE.3.136

COMPLIANCE LEGEND	
	DESCRIPTION
	SCUTE MEETS OR EXECEEDS REQUIREMENTS*
	THIS CONTROL IS NOT ENACTED AT THIS LEVEL

* Compliance standards are not static and constantly revised, as such you must evaluate all systems you integrate against your specific internal standards and the interpretation of your audit body.

C029		RE.2.137 RE.2.138	RE.3.139
C030			
C031		RM.2.141 RM.2.142	RM.3.144
C032		RM.2.143	RM.3.146 RM.3.147
C033			
C034		CA.2.157	
C035		CA.2.158 CA.2.159	CA.3.161
C036			CA.3.162
C037			SA.3.169
C038		SC.2.178 SC.2.179	SC.3.177 SC.3.180 SC.3.181 SC.3.182 SC.3.183 SC.3.184 SC.3.185 SC.3.186 SC.3.187 SC.3.188 SC.3.189 SC.3.190 SC.3.191
C039	SC.1.175 SC.1.176		SC.3.192 SC.3.193
C040	SI.1.210	SI.2.214	
C041	SI.1.211 SI.1.212 SI.1.213		
C042		SI.2.216 SI.2.217	SI.3.218
C043			SI.3.219 SI.3.220

COMPLIANCE LEGEND	
COLOR	DESCRIPTION
	SCUTE MEETS OR EXECEEDS REQUIREMENTS*
	THIS CONTROL IS NOT ENACTED AT THIS LEVEL

* Compliance standards are not static and constantly revised, as such you must evaluate all systems you integrate against your specific internal standards and the interpretation of your audit body.

Cicer One Technologies Inc.

Cicer One Technologies Inc., a data privacy company. SCUTE data privacy and security compliance enabled through decentralized autonomous edge computing. Edge computing offers your business the very latest technology that protects and controls data and users. Decentralized autonomous edge computing removes all third-parties from your data exchange architecture while providing automatic security oversight across users and file management. This Zero-Trust platform controls jurisdictional exposure yet remains globally accessible for secure communications complete with network, user control, data management, and extensive immutable audit control. (www.ciceronetech.com)

Decentralized Autonomous Edge Computing offers embedded AI and operational behavior to reduce the complexity and risk of setup, management, reporting, and file share activities for all user types. Zero-Trust enables information to be protected during storage or exchange across employees including external guests, customers, vendors, or suppliers. Controls on your Edge maintain privacy and security without undesired jurisdictional exposure or third-party service provider exposure. Autonomous operations require only general business skills to easily organize and share files, manage and monitor users, protect intellectual property, and comply with privacy laws.