National Security Prerequisites

Our nation and the protection of its sovereignty is a matter for the federal government and department of defense to enable delivery of practices, procedures, equipment, and weapons. Although the federal government and its various divisions are accountable in the protection of national interest, they generally look to supply everything required through the ingenuity of contracted service providers. These are public and private corporations that bid on contracts and provide confidence to the federal government in the delivery and quality of the contracted activity.

The particulars of any contract will contain information that is intended to remain in control and only be seen by those authorized, contracted, or required to know in order to deliver the contract as per its terms and conditions.

The protection and control of defense related information, designs, specifications, contracts, and final product is imperative to meet the Arms Export Control Act and comply with international agreements and treaties to uphold international law and manage the global proliferation of military technology.

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. Data as property was clearly distinguished.

International Traffic in Arms Regulations (ITAR)

International Traffic in Arms Regulations control the export and import of defense-related articles and services on the United States Munitions List (USML). According to the U.S. Government, all manufacturers, exporters, and brokers of defense articles, defense services, or related technical data must be ITAR compliant.

Digital Information and ITAR Compliance

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.

As a result, ITAR can pose challenges for global corporations, since data related to specific technologies may need to be transferred over the internet or stored locally outside of the United States in order to make business processes flow smoothly. The responsibility lies with the manufacturer or exporter to take the necessary precautions and steps to certify that they are, in fact, meeting ITAR compliance requirements.

This issue is further compounded when a contractor looks across their entire supply chain as the multitude of suppliers often fail to ensure the required level of digital privacy in the collection, exchange, backup, and user management in their facility.

ITAR Digital Data Security Controls

Regarding the digital information your business will receive, transmit, and store, it is important to understand how to secure your ITAR related data. While there are numerous establish cybersecurity hygiene protocols such as National Institute of Standards and Technology (NIST) 800.171, data security will have different requirements for each company. When it comes to your company securing ITAR digital data the following outlines some key best-practices:

- Develop and maintain an information security policy
- Build and maintain a secure network, maintain a firewall configuration
- Avoiding the use of system default or vendor-supplied passwords
- Ensure a traceable and unique ID to each individual with systems access
- Regularly test security systems and employee training
- Protect data in-transit and at-rest with encryption
- Implement controlled and protected system access controls
- Track and monitor all access and actions by all uses upon all data

This list offers a starting point to building a secure ITAR compliant digital asset and user management solution for securing sensitive data.

Violations and National Security Impact

ITAR violations can be harmful to the national security, foreign policy, and adversely impact international stability. The digitization of contract information, specification, details, plans, and other intellectual property and its transmission, storage, and processing creates an immense attack-surface upon which national, foreign or state actors monitor and infiltrate systems in your office and across your supply-chain.

Cybersecurity hygiene is critical in your company and across your supply network. ITAR violations may result in civil penalties, criminal penalties, and other costs such as loss of reputation and revocation of export licenses.

To ensure compliance with the ITAR, the Directorate of Defense Trade Controls strongly encourages registered exporters, manufacturers, brokers, and others engaged in defense trade, to maintain compliance programs that assist in the monitoring and control of exports and other regulated activities.

Enabling ITAR Digital Data Control 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.

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. For the vast majority of subcontractors SCUTE product offers a simple compliance solution for any business. Cost effective and simple is critical especially for subcontractors where their ITAR related business may only be 10-40% of their total revenue.

SCUTE ITAR Compliance

CONTROLS	Compliance
System access control	
Control remote system access	
Data access by authorized user	
User and System Audits	
Control authentication security	
Disaster Recovery implementation	
Control supply-chain data exchange	
Protect data from breach & exposure	
Control foreign jurisdiction exposure	
Control third-party service exposure	
Monitor User Access	
Terminate Dormant User Access	
Encrypt data in-transit & at rest	
Rotate encryption certificates	
Traceability of encryption certificates	
Ensure data stored in country	

COMPLIANCE LEGEND	
COLOR	DESCRIPTION
	SCUTE MEETS OR EXECEEDS REQUIREMENTS

Cicer One Technologies Inc.

Cicer One Technologies Inc., a data privacy company. Cicer One's flagship hardware product SCUTE ushers in a new market segment of *Sealed System Technology* in IT that offers businesses a ransomware safe, globally accessible secure digital asset management and communications platform, complete with user management and full system audit reporting. (www.ciceronetech.com)

Sealed System Technology offers Embedded AI and Operational Behavior codified against Business Operations so Users and Systems are managed against generally accepted business practices. This device truly drives digital asset management automatically, to the benefit of the corporation.

Digital information is managed and exchanged maintaining privacy and data as property ownership while removing all third parties or foreign exposure from the data transaction scheme Applying only general business skills you are able to easily organize and share files, manage and monitor users, protect intellectual property, and comply with privacy laws.