CSOI
CYBERSECURITY OPERATIONS INFRASTRUCTURE

IMPRES
Technology Solutions, Inc.

Executive Order 14028

Capabilities for IT, IOT, IIoT and OT

Pushes agencies to enhance cybersecurity and software supply chain integrity.

Moves the Federal government to secure cloud services, zero-trust architecture, and mandates deployment of multifactor authentication and encryption within a specific time-period.

Why CSOI
(Cybersecurity Operations Infrastructure)

1. Cyber intrusion does not expose an CSOI Provisioned-Trusted infrastructure.
2. Encrypt, Segment and Obfuscate IT, OT, IIoT, for any networked thing.
3. Trusted-Provisioned elements can move across network topologies, maintaining crypto-ID, ZTA Policy
4. SIEM/SOAR integration with CSOI API Integration
5. Simple to deploy at scale, with mere mouse-clicks, on existing network infrastructure, day-1.
6. CSOI also protects those things that cannot protect themselves: ICS, SCADA, Pumps, Generators, Valves, Switches, and related...any networked thing.

EO 14028
Why changes are important

- Adversaries are using increasingly sophisticated methods and cyber operations to attack the supply chain, gain access to critical infrastructure, and steal sensitive information.
- Foreign owned or controlled Information and Communications Technology (ICT) products may create vulnerabilities in U.S. Supply Chains.
- IT providers are often hesitant or unable to voluntarily share information about a cyber incident.
- The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cybersecurity.
- The planned FAR rules will ensure contractors keep national security interests in mind by requiring contractors to follow a set of standardized rules when doing business with the Federal government.

Let's Start A Conversation!

800-652-9686
CSOI@imprestechnology.com