Onclave Aligns to the New Executive Order Security Requirements

(updated from May 2021 to May 2022)

Executive Order 14028

Modernizing Federal Government Cybersecurity – Zero Trust Architecture

Beyond reporting, the executive order lays out how the Federal Government should modernize cybersecurity efforts. This includes making strategic investments in technology and personnel to shore up cybersecurity by:

- Adopting security best practices
- Advancing toward Zero Trust Architecture
- Accelerating movement to secure cloud services including SaaS, IaaS, and PaaS solutions

	Onclave TrustedPlatform™
Accelerated adoption of cloud technology	YES
Develop and implement Zero Trust Architecture	YES
Report to OMB and APNSA with plans	YES
Cloud technology and adopt Zero Trust Architecture	YES
Adopt multi-factor authentication	YES
Encryption for data at rest and in transit	YES

Zero Trust Architecture

"Zero Trust Architecture" means a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses.

	Onclave TrustedPlatform™
Security model, design principles and coordinated cyber and system management strategy – acknowledgment threats inside and outside of network	YES
No implicit trust in any one element, node, or service	YES
Continuous verification of the operational picture – real-time information	YES
User full access with only bare minimum needed to perform their jobs	YES
Node is compromised can ensure damage is contained	YES
Constantly limits access and looks for anomalous or malicious activity	YES
Granular risk-based access controls	YES
Security automation throughout all aspects of the infrastructure to protect data real-time within a dynamic threat environment	YES
Least-privilege access – who, what, when where and how	YES