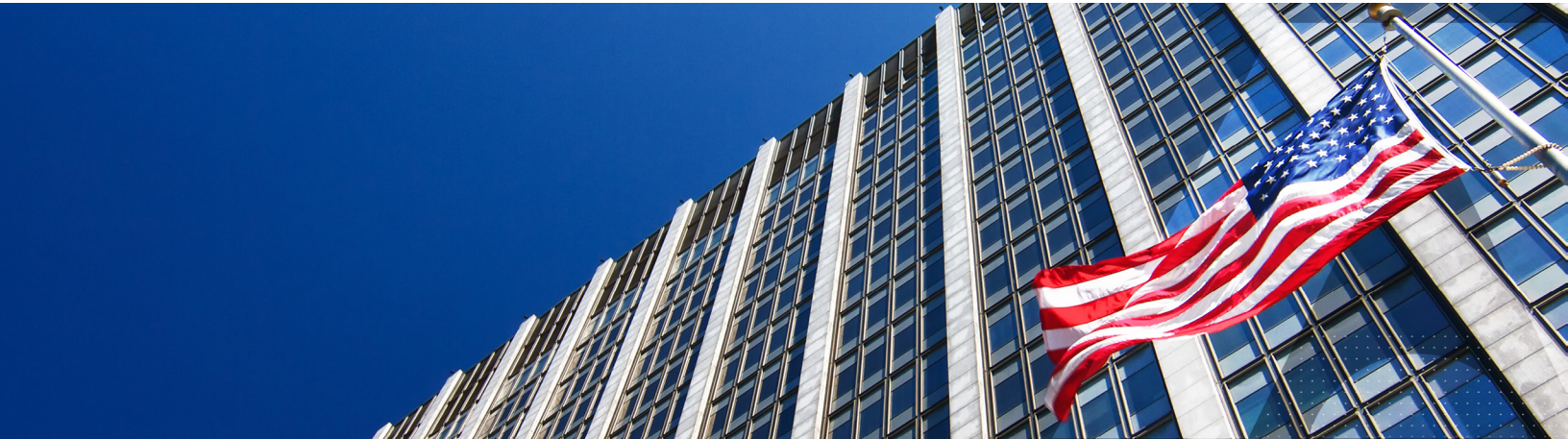# Thales TCT Multi-Factor Authentication & Encryption Solutions for White House Executive Order on Improving the Nation's Cybersecurity

The White House issued an Executive Order on improving the Nation's Cybersecurity on May 12, 2021. The Executive order gives agencies 180 days to "adopt multi-factor authentication and encryption for data at rest and in transit, to the maximum extent consistent with Federal records laws and other applicable laws."

Addressing Modernizing Federal Government Cybersecurity Requirements with Thales TCT Solutions

Thales Trusted Cyber Technologies (TCT) is a U.S. based provider of government high-assurance data security solutions. We offer robust authentication, data at rest encryption, and data in transit encryption solutions that address the requirements outlined in the Executive Order. Our data protection solutions easily integrate within existing IT infrastructures and deliver the same level of security whether deployed in enterprise, tactical or cloud environments. Our solutions enable agencies to meet their immediate data protection needs while investing in a solution that provides robust security, a growing ecosystem, and the scalability needed to build a trusted framework for the future.

Requirement	Why Thales TCT	Thales TCT Solutions
Multi-Factor Authentication Section 3.d of the Executive Order requires the implementation of multi-factor authentication.	From traditional high assurance and commercial-off-the-shelf authentication solutions to first-of-a-kind hardware security module-based identity credentials, Thales TCT offers the most secure, certificate-based authentication platforms available to the U.S. Federal Government.	• **High Assurance Authentication** that brings multi-factor authentication to applications and networks where security is critical. • **Commercial-off-the-Shelf Multi-factor Authentication** offering the broadest range of authentication methods and form factors, Thales TCT allows customers to address numerous use cases, assurance levels, and threat vectors with unified, centrally managed policies—managed from one authentication back end delivered in the cloud or on premise. • **Access Management** through strong authentication services that enable agencies to pursue consistent authentication policies across the organization by automating and simplifying the deployment and management of a distributed estate of tokens, while securing a broad spectrum of resources, whether on-premises, cloud-based, or virtualized.

Requirement	Why Thales TCT	Thales TCT Solutions
Data at Rest Encryption Section 3.d of the Executive Order requires the implementation of encryption for data at rest	Thales TCT offers data at rest encryption solutions that deliver granular encryption and role-based access control for structured and unstructured data residing in databases, applications, files, and storage containers through its CipherTrust Data Security Platform. CipherTrust Data Security Platform unifies data discovery, classification, data protection, and unprecedented granular access controls with centralized key management – all on a single platform. This results in less resources dedicated to data security operations, ubiquitous compliance controls, and significantly reduced risk.	**CipherTrust Data Security Platform** offers a unified data security solution including the following components: • **CipherTrust Transparent Encryption** delivers data at rest encryption, privileged user access controls and detailed data access audit logging. Connectors protect data in files, volumes and databases on Windows, AIX and Linux OS's across physical and virtual servers, in cloud and big data environments. The Live Data Transformation extension, providing zero-downtime encryption and data rekeying. In addition, security intelligence logs and reports streamline compliance reporting and speed up threat detection using SIEM systems. • **CipherTrust Application Data Protection** delivers crypto functions for key management, signing, hashing and encryption services through APIs, so that developers can easily secure data at the application server or big data node. • **CipherTrust Tokenization** is offered both vaulted and vaultless, and can help reduce the cost and complexity of complying with data security mandates. • **CipherTrust Database Protection** solutions integrate data encryption for sensitive fields in databases with secure, centralized key management and without the need to alter database applications. CipherTrust Database Protection solutions support Oracle, Microsoft SQL Server, and IBM DB2 and Teradata databases. • **CipherTrust Manager** centrally manages encryption keys, provides granular access controls and configures security policies. It manages key lifecycle tasks including generation, rotation, destruction, import and export, provides role-based access control to keys and policies, supports robust auditing and reporting, and offers developer friendly REST APIs. CipherTrust Manager also delivers enterprise key management solutions that streamline bring your own keys (BYOK) for multiple cloud environments, supports TDE key management for Oracle and Microsoft SQL Servers, and centralizes key management for a variety of KMIP clients, such as tape archives, full disk encryption, big data, virtual environments and more. • **Luna T-Series Hardware Security Modules** store, protect, and manage cryptographic keys used to secure sensitive data and critical applications. Meeting government mandates for U.S. Supply Chain, the high-assurance, tamper-resistant Luna T-Series HSMs are designed, developed, manufactured, sold, and supported in the United States.
Identifying and Classifying Sensitive Data Section 3.c. of the Executive Order emphasizes the need to "prioritize identification of the unclassified data considered by the agency to be the most sensitive and under the greatest threat".	Thales TCT offers a data discovery and classification solution that enables agencies to get complete visibility of sensitive data with efficient data discovery, classification, and risk analysis across cloud, big data, and traditional environments.	• **CipherTrust Data Discovery and Classification** locates regulated sensitive data, both structured and unstructured, across the cloud, big data, and traditional data stores. A single pane of glass delivers understanding of sensitive data and its risks, enabling better decisions about closing security gaps, prioritizing remediation actions, and securing your cloud transformation and third-party data sharing.
Data in Transit Encryption Section 3.d of the Executive Order requires the implementation of encryption for data in transit.	Thales TCT offers network encryption solutions that provide a single platform to encrypt everywhere—from network traffic between data centers and the headquarters to backup and disaster recovery sites, whether on premises or in the cloud.	• **CN series** network encryptors are hardware network appliances that deliver network layer independent (Layers 2, 3 and 4) encryption for data in tranist. These hardware encryptors are certified for FIPS 140-2 Level 3 and are on the DoDIN APL. • **CV series** is a hardened virtual appliance that delivers robust encryption for data-in-motion across high speed carrier WANs and SD-WAN links, using Network Function Virtualization (NFV).

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., protects the most vital data from the core to the cloud to the field. We serve as a trusted, U.S. based source for cyber security solutions for the U.S. Federal Government. Our solutions enable agencies to deploy a holistic data protection ecosystem where data and cryptographic keys are secured and managed, and access and distribution are controlled. For more information, visit www.thalestct.com

3465 Box Hill Corporate Center Drive, Suite D, Abingdon, MD 21009 • 443-484-7070 • info@thalestct.com
thalestct.com