cpl.thalesgroup.com

THALES
Building a future we can all trust

Thales 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."

Modernizing Federal Government Cybersecurity with Thales Solutions

Thales is a global leader in data protection, trusted by governments and the most recognized companies around the world to help them protect their most sensitive data. We are the only provider that offers robust authentication, data at rest encryption, and data in transit encryption solutions that address the requirements outlined in the Executive Order to help modernize and implement stronger cybersecurity standards in the Federal government. Our data protection solutions enable agencies to Discover, Protect and Control access to sensitive data anywhere and easily integrate within existing IT infrastructures and deliver the same level of security whether deployed on-premises or in cloud environments.

Requirement	Why Thales	Thales 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 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 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	Thales Solutions
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 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 at Rest Encryption Section 3.d of the Executive Order requires the implementation of encryption for data at rest	Thales 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 the 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 fewer resources dedicated to data security operations, ubiquitous compliance controls, and significantly reduced risk. Critical to the success of deploying encryption to protect sensitive information is the security of the encryption keys. In order for the encryption to be effective, the keys should be secured separate from software and stored in a tamper-resistant Luna hardware security module, available on-premises, as a service in the cloud, and across hybrid environments.	**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, available on-premises, as a Cloud HSM service and across hybrid environments. **Luna Hardware Security Modules** generate, 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 HSMs are designed, developed, manufactured, sold, and supported in the United States. Thales Luna HSMs provide a root of trust for existing and emerging technologies including Public Key Infrastructure (PKI), and secure store keys for code signing to maintain code integrity (section 4 (e)(iii). Thales also offers an enterprise custom-tailored code signing solution built on Luna HSMs, containers, and REST APIs, available on-premises, as a Cloud HSM service and across hybrid environments. **Data Protection on Demand (DPoD)** is a cloud-based platform providing a wide range of Cloud HSM and key management services through a simple online marketplace.

Requirement	Why Thales	Thales Solutions
Data in Transit Encryption Section 3.d of the Executive Order requires the implementation of encryption for data in transit.	Thales 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.	**Thales High Speed Encryptors** offer the ideal certified and proven solution for data-in-motion security, including time-sensitive voice and video streams, for enterprise, and government organizations: • 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, Common Criteria, NATO 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

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us