Trusted Cyber Technologies

THALES
Building a future we can all trust

Thales Trust Cyber Technologies Solutions for National Security Memo on Improving Cybersecurity of National Security, Department of Defense and Intelligence Community Systems

The White House issued a National Security Memorandum (NSM) to improve the cybersecurity of National Security, Department of Defense, and Intelligence Community Systems on January 19, 2022. This NSM requires that National Security Systems (NSS) employ the network cybersecurity measures that are equivalent to or exceed those required of federal civilian networks in Executive Order (EO) 14028[1] and gives agencies 180 days to implement multifactor authentication and encryption for NSS data-at-rest and data-in-transit per guidance in Section 3 of EO 14028.

Modernizing Federal Government Cybersecurity Requirements with Thales TCT Solutions

Thales Trusted Cyber Technologies (TCT) is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Federal Government. We offer robust authentication, data at rest encryption, and data in transit encryption solutions that address the requirements outlined in the NSM and EO 14028. Our solutions reduce the risks associated with the most critical attack vectors and address the most stringent encryption, key management, and access control requirements. In addition to our core solutions developed and manufactured in the U.S. specifically for the Government, we sell and support industry-leading, third-party commercial-off-the-shelf solutions. To mitigate the risks associated with procuring data security solutions developed outside of the U.S, we operate under a Proxy Agreement with Defense Counterintelligence & Security Agency (DCSA) for Foreign Ownership, Control & Influence (FOCI) and a Committee on Foreign Investment in the U.S. (CFIUS) National Security Agreement.

As a long-established provider of cybersecurity solutions currently deployed within National Security, Department of Defense, and Intelligence Community Systems, Thales TCT strongly supports the Biden Administration's efforts to raise the bar on cybersecurity. All Thales TCT products currently support the recommended Commercial National Security Algorithms (CNSA) and are being enhanced with quantum resistant algorithms.

Thales TCT stands ready to provide solutions which meet the requirements of the NSM. We are prepared to provide industry input as the Committee on National Security Systems (CNSS) and federal agencies review and update policies as directed in the NSM.

[1] https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/

Requirement	Why Thales TCT	Thales TCT Solutions
Multi-Factor Authentication NSM and EO 14028 Section 3.d require 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. Our High Assurance Authentication products are currently approved for use within National Security Systems.	• High Assurance Authentication that brings multi-factor authentication to applications and networks where security is critical. • Commercial-off-the-Shelf Multifactor 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.
Data at Rest Encryption NSM and EO 14028 Section 3.d require 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 Manager, the central management point for the platform, provides centralized key lifecycle management and policy control, available in FIPS-compliant virtual and physical appliance form factors. CipherTrust Manager can also be rooted to a hardware security module (HSM). Thales TCT T-Series Luna HSM (also embedded in CipherTrust Manager) is specifically approved via CNSS Memo for use in National Security Systems.	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 NSM and EO 14028 Section 3.c. emphasize 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 NSM and EO 14028 Section 3.d require 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. Thales TCT Network Encryptors leverage Quantum Key Distribution (QKD), Quantum Random Number Generation (QRNG) capabilities, and implement Quantum Resistant Algorithms for future-proof data security.	• CN series network encryptors are hardware network appliances that deliver network layer independent (Layers 2, 3 and 4) encryption for data in transit. 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., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the field with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

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