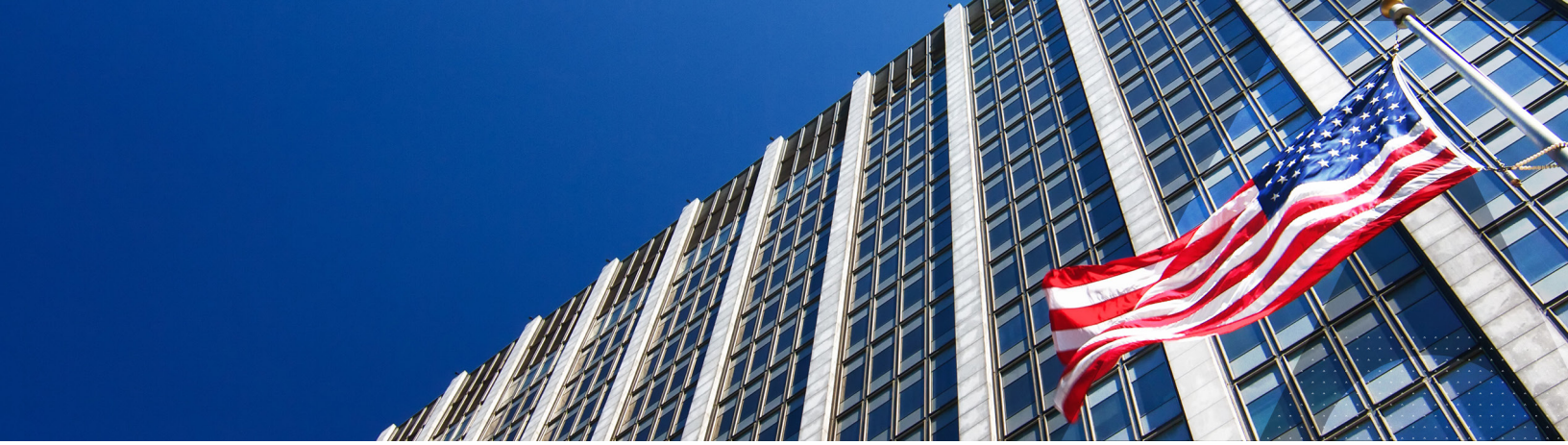
Trusted Cyber Technologies

THALES
Building a future we can all trust

Top Five Ways to Address Requirements in National Security Memo on Improving Cybersecurity of National Security Systems

White Paper

Contents



On January 19, 2022, the White House issued a National Security Memorandum (NSM) to improve the cybersecurity of National Security, Department of Defense, and Intelligence Community Systems. This NSM requires National Security Systems (NSS) to employ the network cybersecurity measures that are equivalent to or exceed those required of federal civilian networks in Executive Order (EO) 140281.

The landmark EO 14028, signed in May 2021, paved the way to implementing new policies aimed to improve national cybersecurity posture. EO 14028 was signed in the wake of several notable cybersecurity catastrophes in 2020 and 2021, such as the ransomware attack targeting the Colonial Pipeline, the Microsoft Exchange server vulnerabilities that affected more than 60,000 organizations, and the SolarWinds hack that compromised many federal agencies.

This NSM builds upon requirements in EO 14028 and raises the bar for the cybersecurity of the U.S.' most sensitive systems. As outlined in the White House fact sheet, this NSM:

- Specifies how the provisions of EO 14028 apply to National Security Systems.
- Improves the visibility of cybersecurity incidents that occur on these systems.
- Requires agencies to act to protect or mitigate a cyber-threat to National Security Systems
- Requires agencies to secure cross domain solutions – tools that transfer data between classified and unclassified systems.

Mapping the NSM to EO 14028

Section 1 of the NSM details the implementation of EO 1428 for NSS and outlines guidance for the:

1. Implementation of multifactor authentication
2. Implementation of encryption for NSS data-at-rest and data-in-transit
3. Application of minimum security standards and controls related to cloud migration and operations
4. Adoption of a Zero Trust Architecture
5. Transition to quantum resistant encryption

This white paper discusses best security practices associated with the aforementioned key components of the NSM. It additionally details how to implement these best practices with solutions from Thales Trusted Cyber Technologies (TCT).

About Thales TCT

Thales TCT 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 edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the most stringent encryption, key management, and access control requirements.

Supply Chain Security

Thales TCT provides U.S. federal agencies with solutions for their cryptographic infrastructure that have a U.S. supply chain lifecycle. Our core data security solutions are developed, manufactured, sold and supported in the U.S.

We additionally mitigate the risk associated with procuring data security solutions developed outside of the U.S. We operate under a Defense Counterintelligence and Security Agency (DCSA) proxy for the protection from Foreign Ownership Control and Influence (FOCI) and are governed by a Committee for Foreign Investment in the U.S. (CFIUS) National Security Agreement for further FOCI mitigation.

Top 5 Ways to Comply with the NSM with Thales TCT Solutions

1. Implementation of Multifactor Authentication

Per NIST SP 800-63, "digital authentication establishes that a subject attempting to access a digital service is in control of one or more valid authenticators associated with that subject's digital identity." For services in which return visits are applicable, successful authentication provides reasonable risk-based assurances that the subject accessing the service today is the same as that which accessed the service previously.
Digital identity presents a technical challenge because this process often involves proofing individuals over an open network, and always involves the authentication of individual subjects over an open network to access digital services. The processes and technologies to establish and use digital identities offer multiple opportunities for impersonation and other attacks.

A system can have strong security if it asks in a systematic manner for multiple authentication factors. This kind of user authentication can have opposite results by jeopardizing user convenience. A good security strategy is one where there is the right tradeoff between security and user convenience, which can be achieved by adapting the level of authentication based on a continuous risk assessment.

Authentication establishes confidence that the claimant has possession of one or more authenticators bound to the credential. Authentication does not determine the claimant's authorizations or access privileges – for example, what they are allowed to do once they have successfully been allowed to access a digital service.
The classic paradigm for authentication systems identifies three factors as the cornerstones of authentication:

- Knowledge factor ("something you know"): The system accepts you if you show that you know a certain bit of information. Examples include PINs, answers to security questions, tax return details, etc.
- Possession factor ("something you have"): The system accepts you if you can prove that you have a certain physical device on you. Examples include devices such as smartcards, mobile phones and USB keys.
- Inherence factor ("something you are"): The system accepts you by using a biometric comparison. Examples include fingerprint scanners, retina scanners, voice recognition, and behavioral biometry.

Multifactor authentication (MFA) refers to the use of more than one of the above factors. The strength of authentication systems is largely determined by the authentication technology deployed and the number of factors incorporated by the system — the more factors employed, the more robust the authentication system. With increasingly complex access environments and more access points than ever before, organizations have every reason to add multifactor authentication.

Multifactor authentication (MFA) refers to the use of more than one of the above factors. The strength of authentication systems is largely determined by the authentication technology deployed and the number of factors incorporated by the system — the more factors employed, the more robust the authentication system. With increasingly complex access environments and more access points than ever before, organizations have every reason to add multifactor authentication.

Thales TCT Multifactor Authentication Solutions

Selecting an authentication method involves maintaining a balance between trust, user experience, and total cost of ownership. However, the process of selecting the appropriate method should involve a structured approach, centered on the need to balance between security and convenience.

From traditional high assurance to commercial-of-the-shelf authentication solutions, Thales TCT offers the most secure, certificate-based authentication platforms available to the U.S. Federal Government.

Certificate-Based Smart Cards & USB Tokens

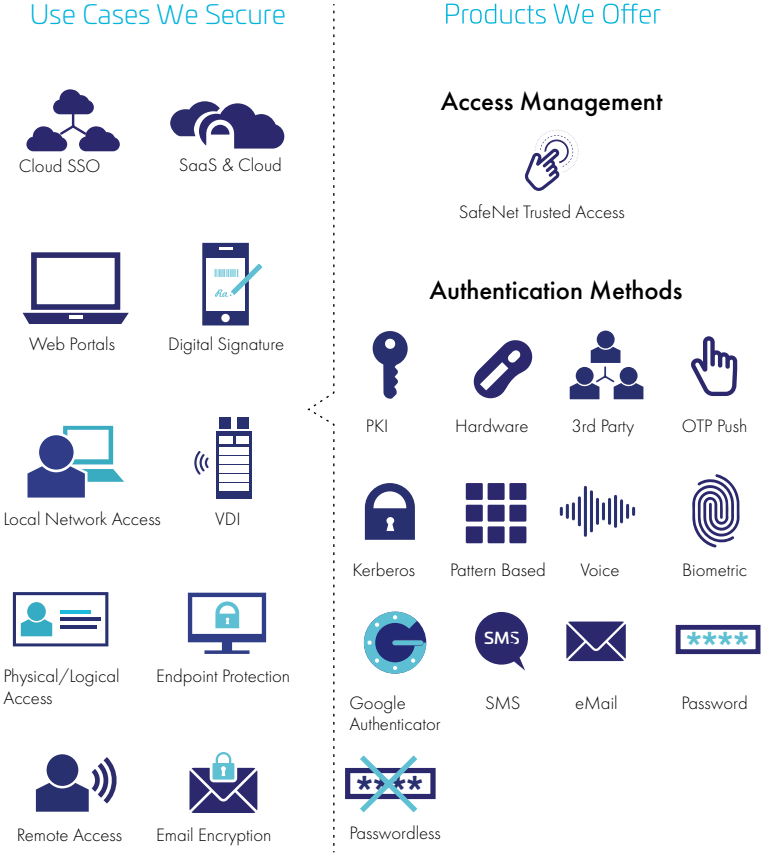
Thales TCT's range of certificate-based smart cards and USB tokens offer strong multifactor authentication and enable agencies to address their PKI security needs. Thales TCT certificate-based authenticators offer a single solution for strong authentication and applications access control, including remote access, network access, password management, network logon, as well as corporate ID badges, magnetic stripes and proximity. Thales TCT's certificate-based authenticators meet the highest security standards, including FIPS 140-2 and Common Criteria (configuration dependent).

FIDO Devices

FIDO authenticators enable multifactor authentication to cloud and web services as well as Windows 10 devices. Thales TCT offers a range of FIDO devices, including a combined PKI-FIDO smart card and a FIDO USB token.

Hardware OTP Tokens

Thales TCT's OTP hardware tokens provide a strong and scalable foundation for securing access to enterprise, web-based and cloud applications, and complying with privacy and security regulations.
The OTP hardware tokens offer rich case-branding options, and are field-programmable by the customer, enabling organizations to maintain stringent control over their own critical OTP security data.



Smartphone and Software Tokens

Offering the convenience of phone-as-a-token authentication, Thales TCT offers PUSH OTP software authentication for tablets and mobile phones.

Tokenless Authentication Solutions

Thales's tokenless technology enables any user to be authenticated anytime and anywhere. Thales's context-based authentication offers convenient, frictionless strong authentication while maintaining the flexibility and agility to add protection with stronger methods of security in higher risk situations. Combined with "step-up" authentication, context-based authentication optimizes a layered approach to access security by assessing user login attributes and matching them against pre-defined security policies.

2. Implementation of encryption for NSS data-at-rest and data-in-transit

Legacy security architectures have failed often and dramatically, because they reflect outdated views of how organizations interact with their data. Data security today needs to recognize not only that data is the most valuable asset of the organization, but also that it is ever-proliferating exponentially.

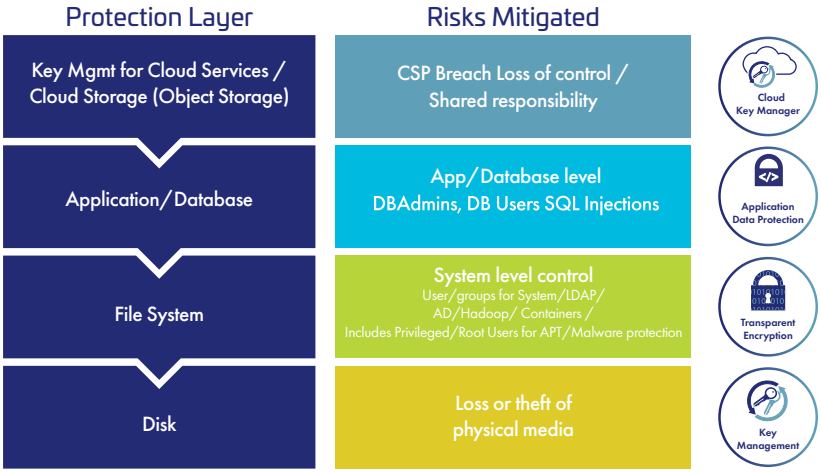
A data-centric approach to security protects the data itself rather than just the endpoints, networks, and applications it moves between. Consequently, the data itself is secure, so it can move as much as the organization needs it to without increased risk. Instead of slowing down progress and inhibiting the proliferation of data, data-centric security empowers the organization to make the most of its data wherever it's stored and used.

Data-at-Rest Encryption

With cyber-attacks on the rise, agencies require the ability to limit access to sensitive information to only those users, groups, and processes that require the use of the data – and no more. This need extends across traditional data centers, cloud environments, SaaS implementations, and to the data stores of every environment. What is required is a way to make sensitive data useless (and valueless) when not in use and then to control access to the make the data accessable when it is needed by a legitimate user. This is what data-at-rest encryption with user access control does. When determining which type of data encryption will best meet your requirements, there are several considerations.

At a high level, data encryption types can be broken out by where they are employed in the technology stack. There are four levels in the technology stack in which data encryption is typically employed: disk, file system, database, and application. In general, the lower in the stack encryption is employed, the simpler and less intrusive the implementation will be. However, the number and types of threats these data encryption approaches can address are also reduced. On the other hand, by employing encryption higher in the stack, organizations can typically realize higher levels of security and mitigate more threats.

Data-at-rest encryption with privileged user access controls significantly improves security posture and not only protects data at rest, but also encrypted workloads in the cloud. Role-based access policies enable a zero trust architecture by controlling who, what, where, when and how data can be accessed. Granular access controls enable administrative users to perform their duties while restricting access to encrypted data.
For encryption to successfully secure sensitive data, the cryptographic keys used to encrypt and decrypt data must be secured, managed and controlled by your organization and not a third-party solution or cloud provider. As agencies deploy ever-increasing numbers of siloed encryption solutions, they find themselves managing inconsistent policies, different levels of protection, and escalating costs.



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 must be secured separate from software and stored in a centralized key manager integrated with a tamper-resistant hardware security module.

Thales TCT Data-at-Rest Encryption Solutions

Thales TCT offers data-at-rest encryption solutions that deliver granular encryption and role-based access control for structured and unstructured data residing in file servers, databases, applications, and storage containers. With centralized key management and a hardened root of trust with a full U.S. supply chain, agencies can ensure their master keys are protected and data remains secure.

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. The platform includes:

- ***CipherTrust Transparent Encryption*** delivers data-at-rest encryption, privileged user access controls and detailed data access audit logging. Agents 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. Security intelligence logs and reports streamline compliance reporting and speed up threat detection using leading security information and event management (SIEM) systems.
- ***CipherTrust Application Data Protection*** delivers crypto functions such as key management, signing, hashing and encryption services through APIs, so that developers can easily secure data at the application server or big data node. The solution comes with supported sample code so that developers can move quickly to secure data processed in their applications. CipherTrust Application Data Protection accelerates development of customized data security solutions, while removing the complexity of key management from developer responsibility and control. In addition, it enforces strong separation of duties through key management policies that are managed only by security operations.
- ***CipherTrust Tokenization*** is offered both vaulted and vaultless and can help reduce the cost and complexity of complying with data security mandates. Tokenization replaces sensitive data with a representative token, so that the sensitize data is kept separate and secure from the database and unauthorized users and systems. The vaultless offering includes policy-based dynamic data masking. Both offerings make it easy to add tokenization to applications.
- ***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, IBM DB2 and Teradata databases.
- ***CipherTrust Manager*** is the central management point for the platform. It 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 databases such as 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.
- Our enterprise key management solutions can utilize a FIPS 140-2 Level 3 validated ***Luna T-Series Hardware Security Module*** as a root of trust. 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.

Data-in-Transit Encryption

Organizations have become dependent upon the fixed, high-speed data networks that serve as its core network infrastructure; providing Big Data, Cloud, SaaS and other digital transformation technologies. These critical technologies and applications generate huge volumes of data that is often transmitted across Wide Area and Metro Area Networks.

The is often a presumption fiber-optics used in core network infrastructure, such as high-speed Ethernet networks, are inherently safe. They are not. Whether a network infrastructure is carrier-provided (public) or government-owned (private), it could be carrying large volumes of data, streamed at anything from 10Mbps to 100Gbps. As a result, it is a high-value target for eavesdropping and all manner of cyber-attacks.

When it comes to protecting core data networks, the risk is even greater. The vulnerabilities present in major vendors' network devices (such as routers and switches) place an additional burden on infrastructure managers who are already under pressure to ensure maximum network uptime and meet application performance requirements.

Ultimately, no organization should depend on data network devices for effective data security; nor should they depend upon low-assurance network devices with embedded encryption. These face similar security and operational weaknesses.

To achieve both maximum encryption security and network performance objectives, core network data must be protected by high-assurance, dedicated hardware encryptors.

Thales TCT Network Encryption Solutions

Thales TCT's comprehensive network encryption solutions support Layer 2, 3, and 4 encryption to ensure security without compromise. Ensuring maximum throughput with minimal latency, our solutions allow customers to better protect data, video, voice, and metadata from eavesdropping, surveillance, and overt and covert interception.

- ***CN9000 Network Encryptors***: Delivering 100 Gbps of high assurance and secure encrypted data, the CN9000 Series provides mega data security (100 Gbps), with the lowest latency in the industry (<2µs).
- ***CN6000 Network Encryptors***: Offering variable-speed licenses from 100 Mbps to 10 Gbps. The CN6140 has a multi-port design that makes this encryptor variable, with speed licenses up to 40 Gbps (4x10 Gbps), highly flexible and cost effective.
- ***CN4000 Network Encryptors***: Versatile and compact, offering 10 Mbps-1 Gbps encryption in a small-form factor (SFF) chassis. The CN4000 series is ideal for branch and remote locations, offering high-performance encryption, without comprising network performance.
- ***CV1000 Virtual Encryptor***: The first hardened virtual encryptor, is instantly scalable and may be deployed rapidly across hundreds of network links, providing robust encryption protection for data-in-motion. The Thales CV1000 Virtual Encryptor is a Virtual Network Function (VNF) that delivers an agile network and reduces capital expenditure requirements. Ideal for organizations that are virtualizing network functions and taking advantage of Software Defined Networking (SDN).

3. Application of minimum security standards and controls related to cloud migration and operations

The Cloud Security Alliance emphasizes the importance of shared responsibility in its latest Security Guidance v4.0. Shared responsibility means that Cloud Solution Providers (CSPs) own the responsibility to secure the infrastructure that runs their cloud services. Data owners are responsible for protecting the confidentiality, integrity, and availability of their data in the cloud.

Securing data in the cloud properly requires that data owners own—and can prove that they own—their data, from inception to deletion. That means that data owners—not their cloud provider—must protect their sensitive data by deploying a cloud security ecosystem where data and cryptographic keys are secured and managed, and access is controlled.

Cloud Security Best Practices

Federal agencies can ensure that their data is properly protected in the cloud by applying the following cloud security best practices.

- Data owners need to directly manage, if not own, their encryption to ensure that their data is protected as it is stored in and moves to and from the cloud.
- Data owners need to own the generation and administration of the cryptographic keys used to encrypt data in the cloud.
- Data owners need to ensure that only validated and authorized users can access sensitive data in the cloud.

Section 1 (b) (i) & (v)

Section 1 (b) (i)

Committee on National Security Systems (CNSS) shall develop and publish guidance, in addition to CNSS Instruction 1253, regarding minimum security standards and controls related to cloud migration and operations for NSS taking into account migration steps that the National Institute of Standards and Technology (NIST) within the Department of Commerce has outlined in standards and guidance.

Section 1 (b) (v)

Develop a framework to coordinate and collaborate on cybersecurity and incident response activities related to NSS commercial cloud technologies that ensures effective information sharing among agencies, the National Manager, and Cloud Service Providers (CSP).

Depending on the sensitivity level of the data stored in the cloud, agencies may choose to deploy either just a few or even all of the aforementioned best practices. However, managing data security across multiple clouds with different cloud storage options quickly gets complex. Therefore, data owners need cloud independent security solutions that can be applied across private, hybrid, public, and multi-cloud environments.

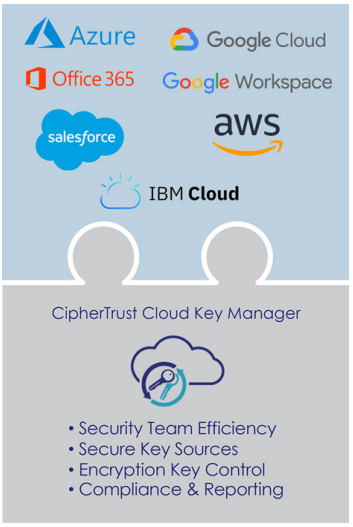
Thales TCT Cloud Data Protection Solutions

Thales TCT offers cloud independent encryption and key management solutions that enable federal agencies to safely store sensitive data in the cloud. Our solutions allow users to effectively manage their security when working in different environments, across different platforms, and with multiple cloud providers. Our cloud data protection solutions can be deployed in public clouds including AWS, Azure, Google Cloud, and IBM Cloud as well as in private or hybrid cloud infrastructures.

Bring Your Own Key (BYOK)

For cloud deployments where security is less critical, agencies may choose to rely on a CSP's native encryption and deploy BYOK services. BYOK services enable users to separate key management from provider-controlled encryption, offering a crucial layer of separation of duties and control.

The NSM points to NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations, guidance via CNSS Instruction 1253. NIST SP 800-53 r5 states that agencies "must maintain physical control of the cryptographic key when stored information is encrypted by external service provides". This guidance specifically calls out external service providers, such as CSPs, and underscores the additional assurance level that physical control of cryptographic keys brings to an agency.

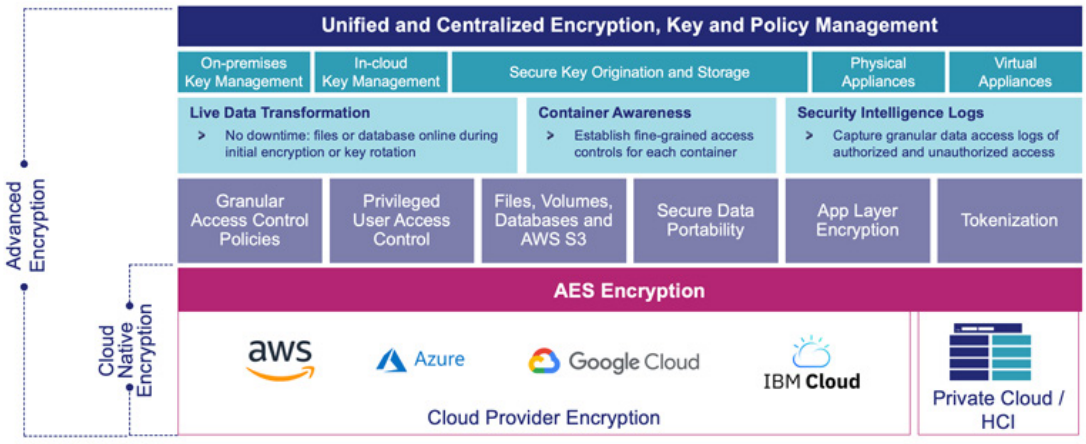


CipherTrust Cloud Key Manager from Thales TCT delivers key generation, separation of duties, reporting, and key lifecycle management that help fulfill internal and industry data protection mandates, with optional FIPS 140-2-certified secure key sources. Both CipherTrust Cloud Key Manager and its key sources are available in all-software, cloud-friendly offerings and may be found in several cloud provider marketplaces for fast instantiation. Further, deployment in any cloud is wholly separated from cloud provider access, and keys can be managed in the cloud in which the solution is deployed as well as any other reachable, supported cloud.

Bring Your Own Encryption (BYOE)

For the highest level of data security in the cloud, users should deploy advanced BYOE tools in their cloud environments. Thales TCT offers advanced multi-cloud BYOE tools through CipherTrust Data Security Platform to secure data and rapidly reach compliance. Compared to the native encryption solutions available from cloud providers, Thales TCT BYOE through CipherTrust Data Security Platform delivers:

- High-performance AES encryption enhanced by hardware acceleration and granular access control policies, including privilege user access control. BYOE controls who, through what process and at specified times, can see specific data.
- An architecture that secures unstructured files, structured databases, and big data environments and also enables users to migrate data between cloud environments and on-premises servers without the time and cost of decryption.
- Easily add tokenization, or format preserving or traditional encryption to applications using RESTful APIs or the industry's most powerful and secure encryption libraries for additional granular controls and regulatory compliance.
- BYOE extensions enable use of data during encryption and rekeying operations with patented Live Data Transformation or, to isolate and secure container environments by creating policy-based encryption zones. BYOE monitors and logs file access to accelerate threat detection with Security Intelligence Log integration with popular SIEM tools.
- Simplified key management across on-premises and multi-cloud deployments by centralizing control on CipherTrust Manager.



4. Adoption of Zero Trust Architecture

Zero Trust is a strategic initiative and principle that helps organizations prevent data breaches and protect their assets by assuming no entity is trusted. Going beyond the "castle-and-moat" concept which had dominated traditional perimeter security, Zero Trust recognizes that when it comes to security, trust is a vulnerability. Traditional security considered all users trusted once inside a network—including threat actors and malicious insiders.

By eliminating the concept of a "safe" network, Zero Trust requires strict identity verification and moves the decision to authenticate and authorize closer to the resource. The identity of the user/device/service provides key context for the application of access policies. With Zero Trust, access rules are as granular as possible to enforce least privileges required to perform the requested action.

While the NSM highlights NIST SP 800-207 Zero Trust Architecture guidance, it is important to note that the U.S. Federal Government has issued additional publications on Zero Trust such as Office of Management and Budget Zero Trust Strategy, Department of Defense (DoD) Zero Trust Reference Architecture, National Security Agency (NSA) Embracing Zero Trust Security Model, and Cybersecurity & Infrastructure Security Agency (CISA) Zero Trust Maturity Model.

CISA's Zero Trust Maturity Model utilizes concepts found in NIST SP 800-207 and DoD and NSA's publications and also highlights requirements in EO 14028. CISA's model "represents a gradient of implementation across five distinct pillars"—Identity, Device, Network, Application Workload, and Data.

Section 1 (b) (ii) (A) & (B)

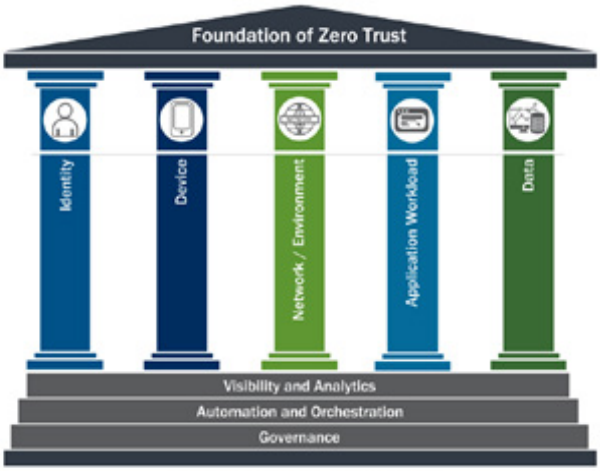
Section 1 (b) (ii) (A)

Update existing agency plans to prioritize resources for the adoption and use of cloud technology, including adoption of Zero Trust Architecture as practicable;

Section 1 (b) (ii) (B)

Develop a plan to implement Zero Trust Architecture, which shall incorporate, as appropriate:

- NIST Special Publication 800-207 Guidance (Zero Trust Architecture);
- CNSS instructions on Zero Trust Reference Architectures; and
- Other relevant CNSS instructions, directives, and policies regarding enterprise architectures, insider threats, and access management



Source: CISA Zero Trust Maturity Model. This illustration was inspired by Figure 1 of the American Council for Technology (ACT) and Industry Advisory Council (IAC) "Zero Trust Cybersecurity Current Trends," (2019)

Thales TCT Solutions for Zero Trust

Thales TCT offers authentication, encryption, and key management solutions that address foundational components of building an effective Zero Trust Architecture.

Identity

Identities are the cornerstone of a Zero Trust Architecture. The CISA defines identities as "an attribute or set of attributes that uniquely describe an agency user or entity. Agencies should ensure and enforce that the right users and entities have the right access to the right resources at the right time".

Thales TCT Authentication and Access Management Solutions

From traditional high assurance and commercial-of-the-shelf authentication solutions to first-of-a-kind hardware security module-based identity credentials for non-person entities, Thales TCT offers the most secure, certificate-based authentication platforms available to the U.S. Federal Government supporting the latest and evolving protocols and standards including WebAuth and FIDO. For more information on Thales TCT's Authentication and Access Management solutions, refer to previous section: *"Thales TCT Multifactor Authentication Solutions" on page 5.*

Device

The integrity of devices connecting to agency networks—whether agency-owned or bring-your-own device (BYOD)—must be validated. Unauthorized devices must be prevented from accessing agency networks and data.

Thales TCT Luna T-Series Hardware Security Modules (HSMs)

Whether the solution involves device attestation, trusted platform modules, secure boot, or similar device integrity technologies, there is always a concept of device identity involved. Thales TCT Luna HSMs are a foundational element in all of these solutions by generating secure device identities or cryptographically signing identity-related data.

Thales TCT Luna Credential System for Non-Person Entity Identity Credentials

Luna Credential System (LCS) introduces a new approach to multifactor authentication by maintaining user or non-person entities credentials in a centralized hardware device that is securely accessible by endpoints in a distributed network. It unites the familiarity of certificate-based authentication with the security of a FIPS 140-2 certified HSM. LCS is a multi-purpose, secure credential system ideally suited for an environment in which the endpoints cannot use a traditional small form-factor token. Ideally suited for Robotic Process Automation (RPA) and fully integrated with industry leading RPA vendors such as UiPath and Blue Prism.

Network

CISA suggests that "need to align their network segmentation and protections according to the needs of their application workflows instead of the implicit trust inherent in traditional network segmentation" and cites encryption as a key ZTA functionality.

Thales TCT Network Encryption Solutions

Thales TCT's network encryption solutions offer high-assurance encryption though secure, dedicated encryption devices that feature embedded, zero-touch encryption key management, end-to-end, authenticated encryption and use standards-based algorithms.

Thales TCT network encryptors are as available a virtual appliance or as hardware-based, stand-alone appliances ranging in performance from 100 Mb to 100 Gb. Thales TCT network encryptors are suited for environments including:

- Big Data Applications
- Data Center Interconnect
- 'Mega Data' Campus Network Environments
- Cloud Computing Services 'Backbones'
- Aggregating High-Speed Network Links
- Large Scale, MAN and WAN Security

Application Workload

CISA recommends that agencies "integrate their protections more closely with their application workflows to ensure the protections have the visibility and understanding needed to provide effective security".

Thales TCT Access Management Solutions

Thales TCT's access management solutions protect applications and the data behind them by ensuring the right user has access to the right resource at the right level of trust. Agencies can control access by setting granular policies so authorized individuals can do their jobs efficiently and effectively. Agencies can monitor user access permissions and the risks associated with each login, applying step-up authentication only when the user's context changes and the level of risk is concerning.

Thales TCT CipherTrust Data Security Platform
CipherTrust Data Security Platform is an integrated suite of data-centric security solutions that unifies data discovery and classification, data protection, and provides unprecedented granular access controls, all with centralized key management.

Thales TCT CipherTrust Application Data Protection for DevSecOps
CISA also recommends that agencies apply zero trust principles to the development and deployment of applications. CipherTrust Application Data Protection supports the rapidly evolving needs of DevOps and DevSecOps, targeting the desired combination of rapid software evolution with security. It offers simple-to-use, powerful software tools for application-level key management and encryption of sensitive data. The solution is flexible enough to encrypt nearly any type of data passing through an application. Application-layer data protection can provide the highest level of security, as it can take place immediately upon data creation or first processing and can remain encrypted regardless of its data life cycle state – during transfer, use, backup or copy.

CipherTrust Application Data Protection can be deployed in physical, private or public cloud infrastructure to secure data even when it is migrating from one environment to another, without any modifications to existing encryption or data processing policies.

CipherTrust Application Data Protection is deployed with CipherTrust Manager, an architecture that centralizes key and policy management across multiple applications, environments, or sites. The combined solution provides granular access controls that separate administrative duties from data and encryption key access. For example, a policy can be applied to ensure that no single administrator can make a critical configuration change without additional approval.

Data

Taking a data-centric approach to security is not only a core component of ZTA, but it also critical for any cybersecurity infrastructure. CISA recommends that "agencies should begin to identify, categorize, and inventory data assets". Next, agencies should deploy security solutions to protect the data itself.

Thales TCT Data-at-Rest Encryption
Thales TCT CipherTrust Data Security Platform is an integrated suite of data-centric security solutions that unifies data discovery and classification, data protection, and provides unprecedented granular access controls, all with centralized key management. For more information on CipherTrust Data Security platform, please refer to above section: "**Thales TCT Data-at-Rest Encryption Solutions**" on page 7.

5. Transition to quantum resistant encryption

Fully-fledged, commercial quantum computers will have the power to change computing as we know it, but when this will happen is a subject of much debate. These changes will have a transformative effect on areas including scientific and medical research, economic analysis, AI, Big Data, and many other disciplines which require large volumes of data and complex calculations.

Quantum computers will also have the ability to do harm. The very same computing power that allows complex problems to be solved can, in turn, be applied to undermine cybersecurity.

Today's public key cryptography is based on factorization for RSA algorithms, or discrete log problems with DSA, Diffie-Hellman, and Elliptic-Curve Cryptography (ECC). Although these hard problems are sufficient today, as soon as a hacker has access to a quantum computer they will be able to weaken these algorithms with quantum algorithms such as Shor's or Lov Grovers, by breaking them or reducing the strength of the symmetric crypto keys and crypto hashes. As a result, everything we rely on today to secure our connections and transactions will be threatened by quantum cryptography, compromising keys, certificates and data.

Today no quantum computer can run quantum algorithms, but once it does, a multitude of public key-based protocols including TLS / SSL, IPSEC, SSH, Internet of Things (IoT), digital signing and code signing will become vulnerable to eavesdropping and public disclosure as they are not strong enough to resist a quantum attack. No one has a concrete date as to when we will hit the post-quantum era, but there are strong indicators that it will start somewhere between 2023 and 2030. If these dates are in fact true, then in some cases, it might already be too late. For example:

- Root Certificate Authorities (CAs) – are valid from 2028 to 2038 which is well beyond when quantum computing will arrive
- Data Retention Requirements – an enterprise that stores and keeps data safe for a determined period of time for compliance or business reasons must take into account the post-quantum era as it may only be 4 years away
- Code Signing Certificates - most will expire in 2021, but any data you transferred over TLS will be potentially decryptable with perfect forward secrecy
- Document Signing Solutions – anything signed now will not have integrity in the post-quantum era

Section 1 (iv) (B) & (D)

Section 1 (iv) (B)

The NSA shall revise and make available to Chief Information Officers the CNSS Advisory Memorandum 01-07 (Information Assurance Cryptographic Equipment Modernization) and any associated enclosures and relevant references regarding modernization planning, use of unsupported encryption, approved mission unique protocols, quantum resistant protocols, and planning for use of quantum resistant cryptography where necessary.

Section 1 (iv) (D)

Agencies shall identify any instances of encryption not in compliance with NSA-approved Quantum Resistant Algorithms or CNSA.

Quantum Random Number Generation (QRNG)

When generating keys, it is crucial that numbers are seeded from a source that is not vulnerable to bias, or easy to predict. This randomness is already key in today's cryptography, and will become even more so in the quantum era, when quantum computers will be able to ascertain patterns in the fraction of the time it takes their classical counterparts.

QRNGs provide high entropy and generate a true source of randomness by leveraging principals from quantum physics. They operate by firing photons (particles of light) at a semi-transparent mirror and assigning them a value of 0 or 1 depending on if they are absorbed or reflected. Because these photons will behave completely randomly, there is no pattern to be observed as seeds are being generated.

Quantum Key Distribution (QKD)

Once cryptographic keys are generated, they must be distributed in a way that guarantees forward secrecy, and thus data integrity. QKD does just this by distributing keys via photons across an optical link. The technology uses another property of quantum physics, known as the 'observer effect', to verify the security and authenticity of these distributed keys.
In practical terms, this means that if a cyber criminal attempted to intercept a key being carried using QKD (via a wire tap for example) the intended recipient would be alerted that it had been observed or tampered with, and thus is not safe to use. In turn, this will give the sender and recipient the chance to generate a new key before any sensitive data is transmitted using the compromised one.

Quantum Resistant Algorithms (QRA)

QRAs are algorithms which themselves are designed to remain secure in a post-quantum world. NIST is currently in the process of finalizing which QRA will go to standardization with a target completion goal of 2024. Once standardized, the current generation of encryption algorithms will need to be replaced with these new quantum-resistant algorithms. This will ultimately require an update to all software and hardware.
NIST guidelines recommend adopting a hybrid classic/quantum state in anticipation of the new standards.

Thales TCT Crypto Agile Solutions for Post-Quantum Crypto (PQC)

The best defense against the quantum threat is crypto agility. NIST's Getting Ready for Post-Quantum Cryptography White Paper states that " Many information systems lack crypto agility—that is, they are not designed to encourage support of rapid adaptations of new cryptographic primitives and algorithms without making significant changes to the system's infrastructure. As a result, an organization may not possess complete control over its cryptographic mechanisms and processes so that it can make accurate alterations to them without involving intense manual effort."

Crypto agility provides you with the ability to quickly react to cryptographic threats by implementing alternative methods of encryption. As a result you will:

- Have the agility to respond to incidents
- Have a definitive inventory of all certs and keys from all issuing authorities
- Know how you are using your keys
- Be able to automate management of server/appliance trust stores and key stores
- Allow for remote updating of device roots, keys, and certificates
- Ensure your PKI can be quickly migrated to new post-quantum resistant PKI root and new algorithms

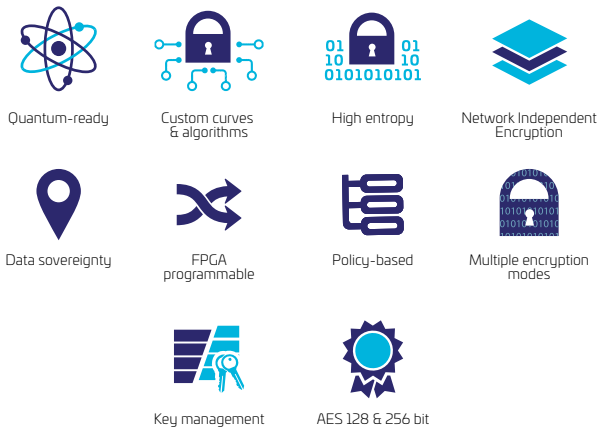
Thales crypto-agility

Thales TCT offers Crypto Agile solutions that offer the following benefits:

- The ability to quickly modify underlying crypto primitives
- Flexible upgradeable technology
- No built-in obsolescence

Our solutions enable users to take a hybrid approach to PQC by using both classic and quantum-resistant crypto in their infrastructure.
Thales TCT Luna Hardware Security Modules, and Thales TCT High Speed Encryptors are crypto agile by design. They enable the most seamless, trustworthy and cost-effective method of transitioning to quantum-safe security while maintaining backward compatibility with existing systems.

The components of crypto-agility



Thales TCT Luna T-Series Hardware Security Modules

The Luna T-Series HSMs provide a crypto agile architecture that supports in-field introduction of new crypto algorithms. In addition, the HSM's crypto module offers large amounts of memory to support growth to larger key sizes. The HSM's CPU capabilities support new, compute intensive algorithms and features.

Quantum Enhanced Keys

By embedding a QRNG chip within the Luna HSM, Thales TCT is offering the industry's first FIPS 140-2 compliant HSM capable of generating quantum enhanced keys. Using principles of quantum physics, the QRNG chip produces high quality entropy which is the basis for all random numbers and cryptographic keys generated by the HSM. With a choice of operating the HSM in FIPS-approved mode using either the embedded, classic physical RNG or the embedded quantum RNG, customers can dynamically change between classical key generation and quantum enhanced keys as threats emerge over time.

Thales TCT High Speed Encryptors (HSE)

Thales TCT High Speed Encryptors are quantum-ready. Thales HSE solutions come with AES 128 and 256 bit standards-based algorithms by default. However, in some circumstances, customers may choose to customize their encryptors with user-defined (or alternative standards-based) algorithms or custom curves for elliptic curve cryptography.

For secure operations, Thales HSEs use true hardware Random Number Generators (RNGs) but also enable customers to incorporate external sources of entropy, such as QRNGs.

Flexibility is another key component of crypto agility. Thales HSEs leverage Field-Programmable Gate Array (FPGA) versatility to both accelerate their time to market and enable simple after-market customization, without the need to update the hardware. The use of FPGA technology provides, in-field flexibility, ease of management and reduces the TCO, improving the returns on any investment in hardware devices.
Flexible deployment is supported by the ability to set simple policies to manage encryption across the network. Truly agile solutions allow these policies to be set based on a variety of criteria, including VLAN ID or MAC address.

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 edge 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