

Best Practices for Implementing the White House Executive Order on Improving the Nation's Cybersecurity Infrastructure



Contents

3	Executive Summary
4	Introduction
4	Zero Trust Architecture
5	Securing Cloud Services
5	Supply Chain Security
5	Thales Solutions for Modernizing Federal Government Cybersecurity
6	Multi-Factor Authentication
7	Data at Rest Encryption
7	Detect Threats and Issue Alerts
8	Secure Cryptographic Keys
8	Identify and Classify Sensitive Data
9	About Thales



Executive Summary

The White House Executive Order on Improving the Nation's Cybersecurity Infrastructure underscores the importance of protecting the Federal Government's computer systems. It will result in a massive review of all cyber security practices and establish consistent guidelines which agencies will need to implement in the short, mid and longer term. Various timelines are noted for the completion of this review and the establishment of updated guidelines. However, within the next two to three months, agencies are already required to take immediate actions aimed at rapidly improving cyber security and modernizing Federal IT architectures. These include:

- Within 60 days agency heads will be required to:
 - Update plans to prioritize the adoption and use of cloud technology
 - Develop a strategy to implement Zero Trust security architecture
- Within 180 days, agencies will be required to adopt multi-factor authentication and encryption for data at rest and in transit

In addition, there are also important implications for companies that do business with the federal government and for the private sector in general. Even if this standardized approach will not be mandatory for the private sector generally, as noted in the White House's Executive Order [fact sheet](#), this playbook would "provide the private sector with a template for its response efforts."

Thales is a recognized global leader in data and identity protection, providing federal and state agencies with solutions that meet Zero Trust security principles by protecting and managing their data, identities and intellectual property.

For years Thales has been at the forefront of ensuring Federal and state agencies protect data and identities with its highly secure and innovative encryption, advanced key management, tokenization, multi-factor authentication and access management solutions. Thales is unique in its ability to offer the breadth of solutions required to meet the Executive Order.

This white paper assesses the key requirements outlined in the Executive Order and details how Thales can ensure the successful and timely implementation of Zero Trust, encryption, and authentication security solutions that Federal and state agencies are now required to deploy.



President Joe Biden signed an [Executive Order](#) on May 12, 2021 which paves the way to implementing new policies aimed to improve national cybersecurity posture. The Executive Order was signed in the wake of several notable cybersecurity attacks 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

The Executive Order underscores the importance of protecting the Federal Government’s “computer systems, whether they are cloud-based, on-premises, or hybrid” and extends the scope to include systems that process data and run vital machinery paramount to the nation’s safety. To accomplish this, the Executive Order outlines several decisive steps needed to modernize its approach to cybersecurity including:

- Sec 3: Modernize Federal Government Cybersecurity
 - Adopt Security Best Practices
 - Encrypt data at rest and in transit
 - Employ multi-factor authentication
 - Secure cloud services
 - Advance towards zero trust architecture
- Sec 4: Enhance Software Supply Chain Security
 - Protect integrity of critical software that performs functions critical to trust
 - Employ encryption of data

Zero Trust Architecture

Zero Trust is a strategic initiative and principle that helps organisations prevent data breaches and protect their assets by assuming no entity is trusted. The National Institute of Standards and Technology (NIST) defines Zero Trust as “a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised.”

Zero Trust goes beyond the “castle-and-moat” concept which dominated traditional perimeter security, recognizing that when it comes to security, trust is a vulnerability. Traditional security concepts considered all users trusted once inside a corporate network – including threat actors and malicious insiders. Trust gave them the right to move laterally and freely access or exfiltrate whatever data they were not limited to.

The definition of Zero Trust indicates that its focus is on authentication, authorization, and minimizing implicit trust zones while maintaining availability and providing seamless authentication mechanisms. Access rules are as granular as possible to enforce least privileges required to perform the requested action. In addition, to assume a ‘never trust, always verify’ stance, it is imperative to encrypt data in transit and data at rest.

Starting points for implementing Zero Trust Security:

- **Ensure** access to resources is determined by a dynamic policy, enforced on a per-session basis, and updated based on information collected about the current state of client identity, application/service, and the requesting asset, including other behavioral and environmental attributes
- All communications to resources must be authenticated, authorized, and encrypted
- Authentication and authorization are agnostic to the underlying network
- The enterprise monitors and measures the integrity and security posture of all owned and associated assets
- **Data at rest and in transit is encrypted**
- **Encryption keys are managed and stored separately to the data**

[Read more on NIST guidelines for implementing Zero Trust Security in this White Paper](#)

Securing Cloud Services

According to results from the [Federal Edition](#) of the Thales 2020 Data Threat Report, “74% percent of U.S. Federal Government agencies store sensitive data in Software as a Service applications, 47% store data in Infrastructure as a Service, and 46% store data in Platform as a Service environments.” A key tenet of good security practices in cloud environments is the ‘shared security’ model, which strongly recommends segregating key security capabilities including access security, authentication and encryption, from the data and applications they are designed to protect. In the ‘shared security model’ government agencies should focus on implementing and owning their own access security and encryption solutions. By so doing they will enhance risk management by reducing the threat surface and lower the risk of lateral attacks in complex environments. In addition, agencies are advised to implement solutions that can simplify the data security landscape and reduce complexity across multiple clouds and legacy environments, as well as modern, cloud-based digital transformation technologies.

These include:

- Data security solutions that enable protection of data moving between clouds and out of the cloud to on-premises environments
- Centralized security solutions that orchestrate data security across multiple cloud platforms
- Authentication and access management to ensure secure, yet convenient, access at the login point

Supply Chain Security

The Executive Order directly addresses enhancing supply chain security. Bad actors exploit weak links in the supply chain. Effective immediately, the National Institute of Standards and Technology (NIST) will collaborate with federal agencies, private industry, and academia to develop guidelines that can be used to evaluate software security, include criteria to evaluate the security practices of the developers and suppliers themselves, and identify innovative tools or methods to demonstrate conformance with secure practices. As an industry leader in cryptography, authentication, data security and delivering products via a secure supply chain, Thales collaborates with NIST on several initiatives including cryptographic algorithms and Zero Trust Security.

[Read more on NIST guidelines for implementing Zero Trust Security in this White Paper](#)

Thales Solutions for Modernizing Federal Government Cybersecurity

Section 3 of the Executive Order explicitly states that “within 180 days of the date of this order, agencies shall 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.” Thales a leading provider of government high-assurance data security solutions, offers modern 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 with existing IT infrastructures and deliver the same level of security whether deployed in enterprise, tactical or cloud environments. Our solutions enable federal 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.

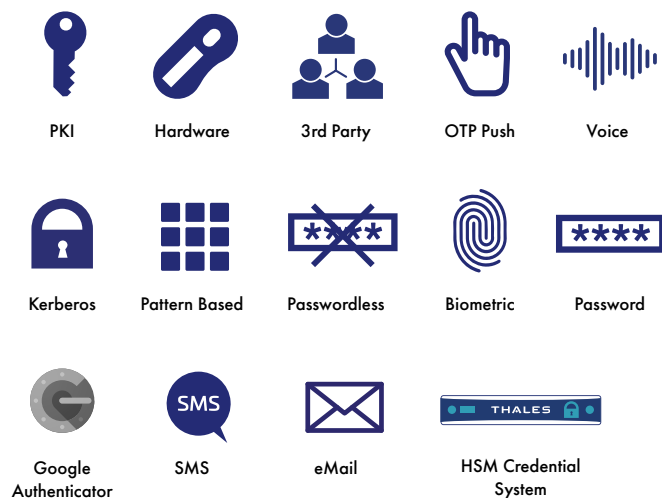
Multi-Factor Authentication

Section 3.d of the Executive Order requires the implementation of multi-factor authentication. Multi-factor authentication ensures that a user is who they claim to be. As Federal and State IT environments move to the cloud and become more complex, traditional security boundaries that in the past protected closed networks are no longer relevant. Identity protection at the access point is the first layer of security and a key to implementing Zero Trust security in distributed and hybrid IT environments. As such, the ability to apply authentication across complex environments which can support cloud and legacy authentication protocols is foundational to modernizing and securing IT environments.

Thales offers the broadest range of [authentication solutions](#) and form factors. Our solutions address numerous use cases, assurance levels, and threat vectors with unified, centrally managed policies—managed from a central platform delivered in the cloud or on-premises.

Thales solutions are flexible and agile and are designed to integrate flexibly and quickly into existing environments within days.

Supported authentication methods include context-based authentication combined with step-up capabilities, Push OTP, OOB, one-time password (OTP), FIDO devices and X.509 certificate-based solutions. All authentication methods are available in numerous form factors, including smart card, USB token, software, mobile app, and hardware tokens.



Thales Authentication and Identity Protection Solutions

From traditional high assurance to commercial- of-the-shelf authentication solutions Thales offers the most secure, certificate-based authentication platforms available. Thales authentication solutions are broadly used by Federal and State agencies in order to protect identities and reduce the risk of credential compromise. They include:

- **High Assurance Authentication** that brings multi-factor authentication to applications and networks where security is critical.
- **Commercial-of-the-Shelf Multi-factor Authentication** that offers 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 platform delivered in the cloud or on premise.
- **Integrated Access Management** and 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.

Access Management



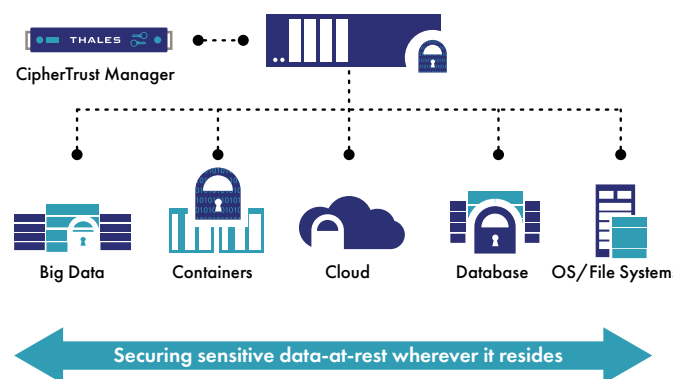
Middleware



Data at Rest Encryption

Section 3.d of the Executive Order requires the implementation of encryption for data at rest. 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.

Thales 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.



Detect Threats and Issue Alerts

Additionally, agencies need awareness of who and what is accessing sensitive data, including privileged users masquerading as other users. Every time a user attempts to access a resource under the protection of Thales's encryption solutions, rich logs of whom, when, where, which policies applied, and the resulting action can be generated.

These logs provide deep visibility into data access, which can be used to alert administrators to unauthorized access attempts to protected data that may represent a threat, and to build typical access patterns when combined with other infrastructure and access information. For instance, a user that typically accesses information in small quantities from within a local network, if seen to be accessing large volumes of data from a remote location, would represent a threat that should generate an alert and be investigated.

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 is available for sale to the U.S. Federal Government exclusively through Thales.

The platform includes:

- **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.
 - **Live Data Transformation Extension** provides zero-downtime encryption and data rekeying.
 - **CipherTrust 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.

Secure Cryptographic Keys

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 tamper-resistant hardware security module.

Thales offers [enterprise key management](#) solutions that enable agencies to manage encryption keys centrally, provide granular access control and configure security policies. Our solutions manage key lifecycle tasks including generation, rotation, destruction, import and export, provide role-based access control to keys and policies, support robust auditing and reporting, and offers developer friendly REST API. Our enterprise key management solutions can utilize a FIPS 140-2 Level 3 validated hardware security module with a U.S. supply chain as a root of trust.



CipherTrust Manager

Identify and Classify 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”. Sensitive data is often spread across on-premises, virtual, and multi-cloud environments.

Thales offers the ability to identify unclassified data via 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 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.
- **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.

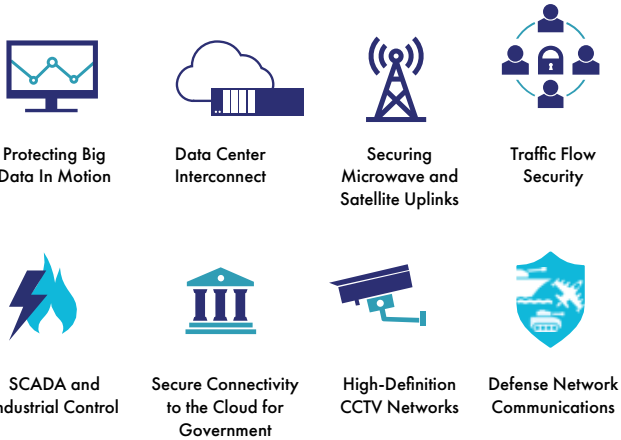
Luna T-Series Hardware Security Modules store, protect, and manage cryptographic keys used to secure sensitive data and critical applications. Meeting government mandates for U.S. Supply Chain, the high-assurance, tamper-resistant Luna T-Series HSMs are designed, developed, manufactured, sold, and supported in the United States.



Data in Transit Encryption

Protecting network transmitted data against cyber-attacks and data breaches is imperative. Section 4.c of the executive order emphasizes encryption of data to enhance the security of the software supply chain. High-assurance network encryption features secure, dedicated encryption devices that protect data in transit. In order to be truly high assurance, these devices must use embedded, zero-touch encryption key management; provide end-to-end, authenticated encryption and use standards-based algorithms.

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. Rigorously tested and certified, our network encryption solutions have been vetted by such organizations as the Defense Information Systems Agency (DISA UC APL) and NATO. Only through Thales’s high-assurance network data encryption can you be assured your data is rendered useless in unauthorized hands and that it will remain secure beyond the data’s useful life.



Thales Network Encryption Solutions

Thales’s comprehensive network traffic encryption solutions use Layer 2 and 3 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. Thales network encryption solutions are available for sale to the U.S. Federal Government exclusively through Thales.

- **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).

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.

THALES

Building a future we can all trust

Contact us

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

> cpl.thalesgroup.com <

