Trustwave®
Government Solutions

# Securing Databases and Complying With Executive Order 14028

Executive Order (EO) 14028 on Improving the Nation's Cybersecurity established several key compliance requirements that agencies must meet as part of their ongoing technology use and adoption. As agencies navigate these new mandates, they need to find solutions that help them put technologies and processes in place to protect their "critical software", including databases.

## 3 Key Requirements for Federal Civilian Executive Branch Agencies

As part of complying with the EO, Federal Civilian Executive Branch (FCEB) agencies face three distinct challenges. Agencies need to modernize their IT stacks, while also securing their supply chains and putting standardized incident response practices in place.

### IT Modernization

As FCEB agencies prioritize cloud strategies, they will need to implement Zero Trust Architectures (ZTA). According to Section 3 "Modernizing Federal Government Cybersecurity" subsection c(iv), they need to create risk-based definitions and categorizations for prioritizing sensitive unclassified data so they can create processing and storage protections.

Agencies often struggle to locate all sensitive data across their complex on-premises and cloud infrastructures. When balancing workforce and financial resource restraints, agencies need cost-efficient solutions that can:

- Discover and identify sensitive data stored in databases
- Track who and what can access the data
- Identify, assess, and remediate vulnerabilities and misconfigurations

## Software Supply Chain Security

Noting the importance of commercial software security in protecting federal networks, the EO explains that the security and integrity of "critical software" is a particular concern.

Within Section 4, the EO outlines the need to establish greater transparency throughout the software development lifecycle. As part of this, it defines three primary actions:

- Adequate controls to prevent tampering
- Mechanisms to ensure secure functioning
- A focus on "critical software" that performs "functions critical to trust," like elevated system privileges or direct networking/computing resource access

Further the EO tasks the National Institute of Standards and Technology (NIST) with:

- Defining "critical software"
- Publishing guidelines for software supply chain security
- Setting standards, procedures, or criteria for securing software development

As agencies work to secure their supply chains, they need to find solutions that augment their current technology investments in ways that reduce the total cost of ownership and security risk.

## Standardized Incident Response Playbook

To ensure consistent incident response activities across federal networks, the EO mandates the creation of standardized response processes to identify, remediate, and recover from vulnerabilities and incidents.

According to the EO, the standard set of operational procedures (playbook) shall:

- incorporate all appropriate NIST standards
- be used by FCEB Agencies and
- articulate progress and completion through all phases of an incident response, while allowing flexibility so it may be used in support of various response activities

Under this section, agencies need to build out their security operations center (SOC) capabilities. SOC teams should look to augment their current endpoint security tools with services that enhance response capabilities. This approach reduces total security costs by enriching current capabilities rather than adding technology redundancies to the security stack.

# How Databases Fit into NIST's EO-Critical Software Mandate

NIST explains in a whitepaper that the word "critical" can be interpreted in various ways. For this reason, the agency decided to use the term "EO-Critical Software" to create a distinction and ensure clarity. Within this meaning, EO-Critical aligns to the definition of a High Value Asset (HVA).

## How does NIST define EO-Critical Software?

Taking a cue from the concept of HVA, NIST's definition of EO-Critical Software focuses on information systems that are so critical to an agency's ability to function that a loss of information, corruption of information, or a loss of access to the system would have a significant negative impact. While EO-Critical Software is not considered an HVA, NIST explains that "EO-Critical Software pinpoints the software that may feed into the HVA systems."

Under the EO, the National Institute of Standards and Technology (NIST) establishes a definition of "critical software." NIST defines EO-Critical Software as any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes:

- is designed to run with elevated privilege or manage privileges
- has direct or privileged access to networking or computing resources
- is designed to control access to data or operational technology
- performs a function critical to trust
- operates outside of normal trust boundaries with privileged access

From a database security perspective, the key phrase in this definition is "direct software dependencies." Fundamentally, databases exist to support other applications by storing the data they need to be effective.

## How do databases fit into the NIST EO-Critical Software landscape?

Reviewing the NIST definition of "direct software dependencies" brings database security within the EO-Critical Software realm.

NIST clarifies the term "direct software dependencies" as "other software components (e.g., libraries, packages, modules) that are directly integrated into, and necessary for operation of, the software instance in question. This is not a systems definition of dependencies and does not include the interfaces and services of what are otherwise independent products."

At their core, databases are "direct software dependencies." Without integrating with databases, on-premises software and Software-as-a-Service (SaaS) applications offer little value. For example, if an agency uses an Enterprise Resource Planning (ERP) application like Oracle ERP, the database connected to the ERP is a direct software dependency.

## Applying the NIST Security Controls for EO-Critical Software to Databases

As agencies seek to secure their EO-Critical Software, they also need to apply the same security measure to their databases. Without securing databases, the applications lack security. If threat actors can use databases as a backdoor into FCEB agency networks, then the agencies have failed to mitigate risk and to comply with the EO's mandates.

This tight integration between databases and software means that agencies need to apply the NIST Security Controls to their databases to ensure holistic security and compliance.

Building on the NIST Cybersecurity Framework and NIST Special Publication (SP) 800-53 "Security and Privacy Controls for Information Systems and Organizations," NIST established a new set of Security Measures (SM) that act as guidelines and best practices.

NIST defines Security Measure as "a high-level security outcome statement that is intended to apply to all software designated as EO-Critical Software or to all platforms, users, administrators, data, or networks (as specified) that are part of running EO-Critical Software."

As agencies work to apply these SMs to their software, they also need to consider where database security fits into their initiatives to ensure compliance with the EO mandates.

# Best Practices for Securing Databases to Comply with the EO Mandate

Database security is mission-critical for agencies as they seek to meet these new compliance requirements outlined by the EO and NIST. With that in mind, understanding the SMs that apply to databases and establishing best practices can make the process less burdensome over the long term.

## Objective 1: Protect EO-Critical Software and EO-Critical Software platform from unauthorized access and usage

The cloud-first and ZTA mandates means that enforcing the principal of least privilege across all resources is fundamental to any agency's security initiative. Agencies need to incorporate database security to mitigate the risk that malicious actors will use databases as a backdoor to gain access to software, systems, and federal networks.

## Controls

Under Objective 1, the following NIST SMs apply to agencies to ensure their databases have the following controls in place:

- SM 1.2: Identify and authenticate each service attempting access
- SM 1.3: Follow privileged access management principles, including hardening platforms and logging all administrative sessions
- SM 1.4: Employ boundary protections, like network segmentation, isolation, and software-defined perimeters

## Best Practices

To secure database access, agencies should:

- Limit user access rights according to the principle of least privilege
- Discover excessively privileged user and service accounts
- Remediate excess access by enforcing principle of least privilege based on role and permissions needed
- Set baselines for acceptable user and service account activity
- Monitor privileged user activity
- Use machine learning to detect anomalous privileged user access to databases
- Respond to alerts, such as terminating queries or counteracting application activities within the database

## Objective 2: Protect the confidentiality, integrity, and availability of data used by EO-Critical Software and EO-Critical Software platforms

EO-Critical Software and EO-Critical Software platforms depend on databases that store the data they need to protect under Objective 2. To ensure consistent protection across software and systems, they need to apply the same security controls to their databases.

### Controls

Under Objective 2, agencies need to ensure their databases have the following controls in place:

- SM 2.1: Establish and maintain a data inventory
- SM 2.2: Use fine-grained access control for data and resources by enforcing the principle of least privilege to the extent possible.
- SM 2.4: Protect data in transit by encrypting sensitive data communications for EO-Critical Software.

### Best Practices

To protect the confidentiality, integrity, and availability of data stored in databases, agencies should:

- Engage in sensitive data discovery across databases to guide user access control and monitoring policies
- Classify sensitive data such as personally identifiable information or protected health information
- Assign and enforce user access accordingly based on presence and location of sensitive data
- Review access controls to maintain principle of least privilege continuously
- Continually audit environment for the discovery of current and new databases

## Objective 3: Identify and maintain EO-Critical Software platforms and the software deployed to those platforms to protect the EO-Critical Software from exploitation

Agencies need to protect their databases from exploitation as part of protecting their data and their EO-Critical Software.

### Controls

Under Objective 3, agencies need to ensure their databases have the following controls in place:

- SM 3.1: Establish and maintain a software inventory that includes cloud-based resources
- SM 3.2: Use patch management practices to prevent exploitation of known vulnerabilities by identifying, documenting and mitigating risks through patching, updating, and upgrading to supported versions

### Best Practices

To protect databases from exploitation, agencies should:

- Continually audit their environment for the discovery of current and new databases
- Automate the identification, assessment and remediation of database vulnerabilities and misconfigurations
- Report on the relationship between the detected risk, vulnerability, or Security Technical Implementation Guide (STIG) impacted
- Remediate the risk, vulnerability, or STIG compliance violation

## Objective 4: Quickly detect, respond to, and recover from threats and incidents involving EO-Critical Software and EO-Critical Software platforms

Securing software and reducing the risk that threat actors will successfully deploy a supply chain attack requires having controls in place that can detect new threats and reduce the time it takes to recover from them. Since databases store the sensitive information that applications and platforms use, agencies need to incorporate database security when complying with the EO mandate.

### Controls

Under Objective 4, agencies need to ensure their databases have the following controls in place:

- SM 4.2: Continuously monitor the database security to detect anomalous activity and new risks
- SM 4.3: Employ endpoint security protection to databases that can:
  - Identify, review, and minimize the attack surface and exposure to known threats
  - Proactively detect threats and stop them when possible

### Best Practices

To detect, respond to, and recover from threats to databases, agencies should:

- Monitor database activity and establish audit trails for all privileged activities
- Enable anomaly detection
- Use machine learning to detect anomalies and new threats

# Database Security to Meet NIST EO-Critical Security Measure Compliance

Trustwave's suite of technology and services solutions offers FCEB agencies a cost-effective way to comply with EO mandates.

## Incorporate Database Security into Zero Trust Architecture Journey

When looking to meet EO mandates, FCEB agencies must consider database security as a fundamental element of their Zero Trust Architecture.

DbProtect is purpose-built and designed for complex data infrastructures. With DbProtect, agencies can:

- Engage in sensitive data discovery and classification
- Scan for vulnerabilities and misconfigurations
- Utilize monthly knowledgebase updates to guide remediation actions to strengthen database security and measure compliance against industry frameworks
- Identify excessively privileged user and service accounts
- Provide visibility into the role of permissions and responsibilities to guide actions to comply with the principle of least privilege
- Monitor database activity with customizable policies based on vulnerability and access rights findings
- Establish audit trails for all privileged activities to aid in breach forensics intelligence

With DbProtect, agencies can gain more control over privileged user access to databases and limit user access to sensitive data according to the principle of least privilege. By setting baselines and using machine learning to detect anomalies, agencies can continuously monitor database activity and remediate access policy violations more efficiently. By controlling and enforcing access policies, agencies follow best practices for ZTA to aid in meeting EO zero trust mandates.

## Enhance Supply Chain Security Across Complex Architectures

Complex agency on-premises and cloud-based infrastructures incorporate multiple database types. Each database requires a different skill set and has a different group of database administrators. However, security teams remain responsible for ensuring security across these divergent technologies.

With DbProtect, agencies can aggregate and correlate security information across different data types, including, but not limited to:

- Oracle
- Microsoft SQL Server
- IBM Db2 (z/OS and LUW)
- SAP HANA and (Sybase) ASE
- PostgreSQL
- MariaDB
- MongoDB
- MySQL
- Teradata
- Percona for MySQL
- Elasticsearch

With DbProtect, agencies can monitor and administer the security measures and findings for their disparate database types in a single location. This reduces the workforce time spent generating scripts and researching database vulnerabilities. By managing all database security with DbProtect, agencies simplify their activities to meet compliance requirements and enhance their ability to go beyond basic compliance activity to ensure their databases are secure and their sensitive data is protected.

## Reduce Total Cost of Ownership (TCO)

Instead of creating technology redundancies, agencies can leverage current security investments and augment them to reduce TCO. By aggregating and correlating disparate database types in a single location, agencies no longer need to spend workforce and financial resources on manual database security measures, such as generating scripts, researching database vulnerabilities, or labor intensive, manual management of user privilege. Most important, security, network, and database administrators can collaborate more effectively to reduce operational costs associated with ensuring the security of their databases and critical software.

DbProtect has over 5000 out-of-the-box security checks against databases, provides monthly knowledgebase updates from the dedicated SpiderLabs database research team, and will reduce agency operation costs by:

- Providing purpose-built insight into the vulnerabilities and threats within structured databases
- Automating the scanning for vulnerabilities and misconfigurations
- Prioritizing vulnerability and misconfiguration actions based on risk
- Pin-pointing the location and classification of the sensitive data within databases so custom monitoring and access controls can be tailored to the riskiest data
- Reporting the relationship between the detected risk and the CVE or Security Technical Implementation Guide (STIG) impacted
- Providing sample remediation script and intelligence from dedicated SpiderLabs researchers to understand how to remediate database weaknesses
- Clarifying user and service account access rights for least privilege access control
- Enabling comprehensive database security without the need for proprietary hardware or the concern of growing license costs as database activity grows

With DbProtect, agencies spend less workforce and financial resources on database security. Moreover, security, network, and database administration teams can collaborate more effectively leading to reduced operational costs and total cost of ownership.

## Engage in a Database Risk Assessment to Protect Sensitive Unclassified Data

To protect sensitive unclassified data and set storage protections, agencies need to identify database risk exposures and compliance postures. As agencies begin the EO compliance process, they need to know the locations of databases and understand their database security.

Trustwave's Database Risk Assessment (DRA) service provides an independent database risk and compliance analysis that includes:

- Database identification within a defined IP range or domain to locate rogue or abandoned databases containing sensitive unclassified data
- Vulnerability assessment scan to detect potential vulnerabilities, or misconfigurations that increase database attack risks
- User Entitlement Review to identify who accesses data and how they obtained rights

## Augment Security team Capabilities with Managed Detection and Response

Improve Utilization of Security Tools and Teams with Managed Detection and Response

As agencies look to improve cyber resilience and comply with the new incident response playbooks, they need partnerships that enable them to get better threat telemetry out of their existing security tools and augment their current security team capabilities with specialized resources like threat analysts, investigators, threat hunters and remote incident responders. Trustwave Managed Detection and Response is a managed service that combines 24x7 threat monitoring with advanced threat detection and incident response.

Trustwave Managed Detection and Response services help agencies achieve effective and timely detection and response outcomes, improve cyber resilience and enable their security resources to focus on more strategic activities. The Trustwave Fusion platform allows agencies to easily integrate existing security tools to synthesize alerts and reduce false positives. Real-time analytics and best-in-class Trustwave SpiderLabs threat intelligence enable our experts to contextualize threats and automate containment actions while they investigate or hunt for threats. We then provide rapid and effective response, informed by agencies' policies and runbooks, and enabled by automation.

We are ready and eager to assist you in your cybersecurity journey. To learn more about Trustwave, please visit www.trustwave.com or contact our team at 1-844-484-7253 and sales@trustwavegovt.com.

## Trustwave for Government Agencies

As agencies develop strategies to comply with the mandates set forth in EO 14028, they need to secure all software defined as "EO-Critical" or as "direct software dependencies." The short EO-defined timelines challenge agencies, especially when looking to secure their riskiest data within their databases and to ensure they implement processes and technology that will move beyond basis security compliance.

Strengthening FCEB agency cybersecurity posture requires a multifaceted approach. Trustwave has experience with aiding FCEB agencies and the private sector. FCEB agencies can work with Trustwave to accelerate their compliance and security maturity by securing their databases and augmenting their current security staffing with MDR services.

Trustwave is recognized as a global security leader for stopping cyberthreats in the hybrid multi-cloud world. With more than 2,000 security-focused professionals operating in 96 countries, Trustwave helps organizations detect and respond to global threats and assists IT teams in meeting strategic and tactical security objectives.

Trustwave SpiderLabs, an elite team of analysts, threat hunters and investigators, operating from a global network of security operations and research centers, investigate malware, web clients and servers, emails, databases, applications and major vulnerabilities.

Unanimously lauded by industry analysts for our strategic vision and ability to execute, Trustwave is relentlessly focused on helping clients stay secure in the digital era. Trustwave is a Singtel company and the global security arm of Singtel, Optus and NCS, with more than 5,000 enterprise clients.For more information, visit *www.trustwave.com.*

Trustwave®
Government Solutions