CYERA

Securing Bulk Transfers of Personal Data

How Cyera Supports Compliance with E.O. 14117

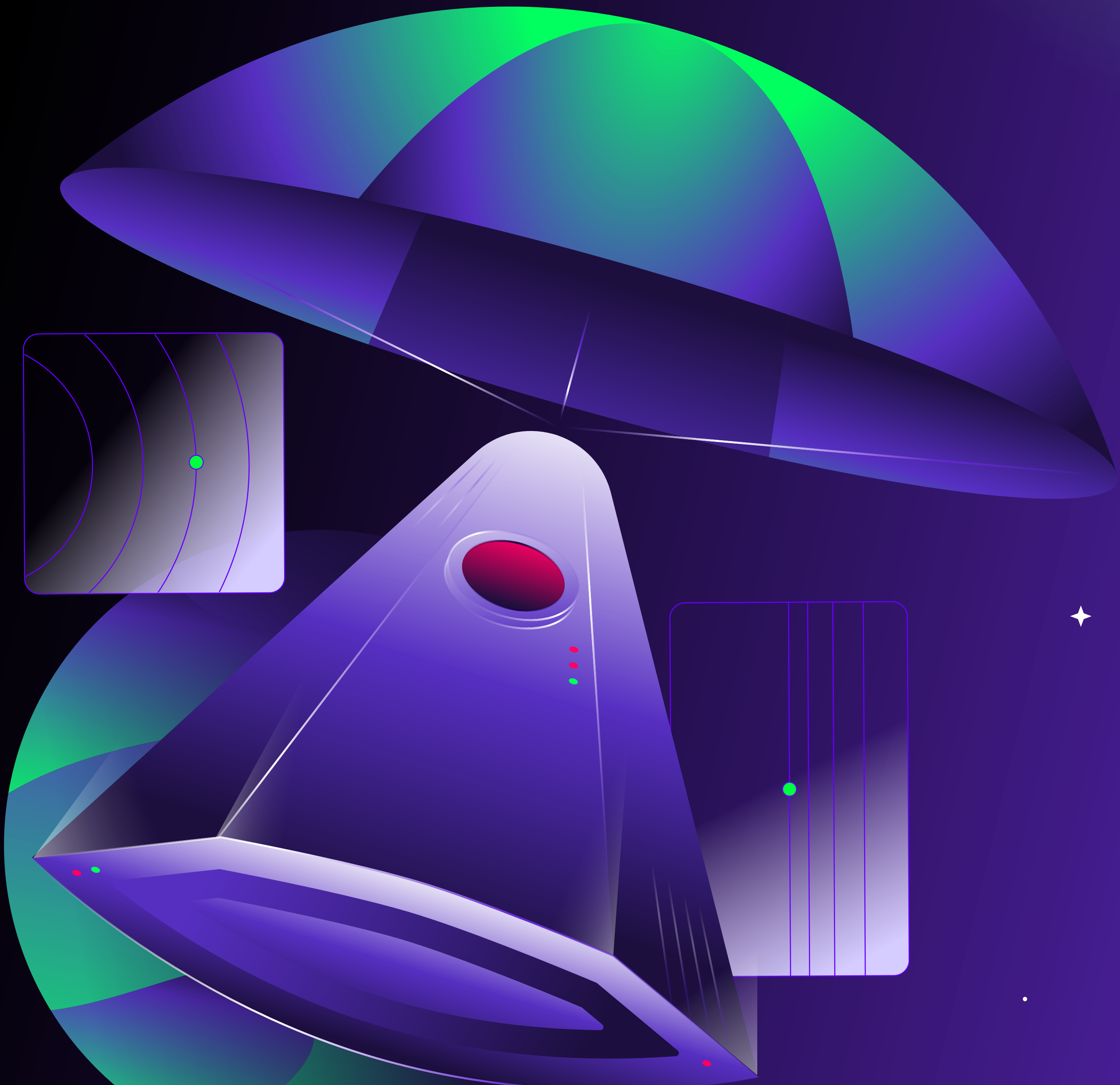

Table of Contents

Introduction

About Executive Order 14117

The purpose of the Order is to prevent America’s adversaries from acquiring data that could be used for espionage, or to train A.I. models that might pose a threat to U.S. national security, or otherwise present a significant risk of harm to the interests of the U.S. government or American citizens.

To that end, the government has prohibited or restricted certain kinds of “covered transactions” - data brokerages, employment agreements, vendor agreements, and investment agreements - that involve bulk quantities of sensitive personal data belonging to certain defined categories. Generally speaking, the more sensitive the data, such as genomic or biometric data, the fewer instances are required to be considered “bulk.”

About Cyera

Cyera is a unified, AI-native data security platform that empowers businesses to discover, classify and protect data. It allows security leaders to manage sensitive data across highly permissive and widely distributed environments with high precision and efficiency.

The platform’s agentless, fully automated data discovery provides a comprehensive inventory of sensitive data across structured and unstructured sources, and across IaaS, SaaS, DBaaS and on-premises environments. This capability enables organizations to address critical data challenges like data proliferation and drift. Powered by AI-native classification, Cyera goes beyond traditional methods by also understanding context, intent, and nuance - decoding data down to the DNA level. This deep insight helps uncover ghost data, reveal sensitive data risks, reduce false positives, and mitigate threats like data breaches and ransomware — areas where conventional data loss prevention and data governance tools fall short.

By combining advanced technology with ease of use, and scale from its cloud-delivered backbone, Cyera empowers organizations to confidently secure their data, maintain compliance, and unlock the full potential of their data to drive innovation.

Organizational Controls

Implementation Requirements	Cyera Capabilities
1. **Continuously identify, prioritize, and document** all covered system assets, maintaining a regularly updated inventory (at least monthly for IT assets) including IP addresses, to ensure comprehensive visibility and tracking of critical system components.	Cyera's AI-native DSPM discovers and classifies all data across SaaS, IaaS, PaaS, DBaaS, and on-prem environments. Cyera automatically inventories sensitive data assets and maps associated data flows, supporting recurring updates and precision tracking of critical system components.
2. **Designate an individual** (e.g., CISO) at the organizational level to be responsible and accountable for cybersecurity and/or GRC functions, ensuring clear ownership of these critical areas.	While the designation itself is the responsibility of the organization, Cyera provides executive-ready risk assessments for GRC and security leaders.
3. **Remediate KEVs** in internet-facing systems within 45 days, prioritizing critical assets. Implement compensating controls if patching isn't feasible, and establish a process to assess pre-patch compromises.	Cyera aids KEV management by surfacing sensitive data exposure in KEV-affected systems and integrating with patch validation workflows through SIEM/SOAR.
4. **Document and maintain** all vendor/supplier agreements for covered systems (e.g., third-party network connection agreements), including contractual IT and cybersecurity requirements.	Cyera’s Identity Access and Omni DLP modules provide visibility into third-party accounts accessing sensitive data, helping validate vendor compliance obligations.
5. **Maintain an accurate network** topology of covered systems and interfacing networks to facilitate visibility into connections between assets, and aid in timely identification of and response to incidents.	Cyera helps maintain up-to-date logical topology by mapping data flows and system interactions across all assets. This supports incident triage and forensic response by providing a real-time, contextual view of connected assets.
6. **Implement a policy requiring approval** for new hardware/software deployment in/on a covered system. Maintain a risk-informed allowlist of approved hardware and software for covered systems.	Cyera supports risk-based hardware/ software allowlists through continuous scanning for unapproved or unmanaged (Shadow IT) assets, alerting security teams to unvetted components within covered systems.
7. **Develop and maintain** incident response plan(s) applicable to covered systems, which should be reviewed annually and updated as appropriate.	Cyera’s Breach Readiness service includes tabletop exercises and dark web OSINT, helping organizations build, validate, and improve incident response plans specific to data exposure risks in covered systems.

Logical and Physical Access Controls

Implementation Requirements	Cyera Capabilities
1. **Enforce multifactor authentication (MFA)** on all covered systems. If MFA is not feasible, require strong passwords (15+ characters) to ensure robust authentication.	Cyera detects users lacking MFA and identifies insecure passwords or weak authentication schemes, enabling policy-based enforcement across the covered system.
2. **Promptly revoke individual** and shared credentials, and authorized access to covered systems, upon termination or change in roles for any individual with access to covered system(s).	Cyera flags stale identities and unrevoked credentials after role changes or terminations, ensuring access rights are rescinded promptly to maintain covered system integrity.
3. **Collect and securely** store access/security logs for covered systems for at least 12 months, using them for detection and incident response. Implement alerts for log source failures and restrict access to authorized users.	Cyera logs sensitive data activity and integrates with SIEMs to enable centralized logging and alerting. Cyera detects log gaps and can escalate when expected log sources go silent, supporting forensics and regulatory retention mandates.
4. **Implement deny-by-default** configurations for all connections to covered systems and their networks, allowing only explicitly approved connections for specific functionalities.	Cyera supports zero trust enforcement by identifying overly broad access and alerting when unauthorized or unexpected connections are established, ensuring adherence to least-privilege access design.
5. **Maintain an accurate network** topology of covered systems and interfacing networks to facilitate visibility into connections between assets, and aid in timely identification of and response to incidents.	

Risk Assessment

1. **Conduct an annual internal** data risk assessment to evaluate and mitigate access to linkable, identifiable, unencrypted, or decryptable covered data by unauthorized entities, considering disclosure likelihood and harm.	Cyera's Data Risk Assessment evaluates the linkability, identifiability, and decryptability of data sets. It delivers mitigation strategies based on classification precision, providing compliance assurance with EO 14117 data handling expectations.

Data Controls

Implementation Requirements	Cyera Capabilities
1. **Implement data minimization** and masking strategies to prevent unauthorized visibility into covered data. This includes maintaining retention policies, processing data to minimize linkability (e.g., aggregation, pseudonymization), and treating related systems as covered systems.	Cyera excels in minimization and obfuscation, detecting redundant, obsolete, or trivial (ROT) data, enforcing deletion policies, and applying masking, pseudonymization, and de-identification techniques to sensitive fields to reduce linkability risks.
2. **Encrypt all covered data** in restricted transactions (in transit and at rest). Securely manage cryptographic keys, ensuring they are not co-located with data, stored in countries of concern, or accessible to unauthorized individuals. Key management systems are covered systems.	Cyera discovers unencrypted data in transit or at rest and flags key management violations, such as colocation with sensitive data. Cyera does not store or manage keys directly but surfaces key exposure risks and validates adherence to encryption policies.
3. **Implement privacy enhancing** technologies (PETs) like homomorphic encryption or differential privacy for covered data. These PETs must prevent unauthorized disclosure or reconstruction of covered data by limiting access to covered persons, even when linking with other datasets. Systems using such processing are considered covered systems.	While Cyera does not implement PETs directly, it monitors AI outputs and linked datasets to ensure PET-wrapped processes don’t inadvertently expose covered data.
4. **Configure the previously** outlined identity and access management techniques to deny authorized access to covered data by covered persons and countries of concern within all covered systems.	Cyera's Identity Access enforces role-based data policies, detecting violations where covered persons or countries of concern are granted access to sensitive data, and supports automatic remediation to restrict access within covered systems.