CYERA

WHITEPAPER

Operationalizing Executive Order 14117: Data Identification and Segmentation with Cyera

How CISOs Can Translate Mandate into Measurable Action

Executive Summary

Executive Order 14117 redefined how organizations handling U.S. persons' data must evaluate, protect, and control that information—especially against foreign access and misuse. For CISOs, it's a mandate for data awareness, segmentation, and governance aligned to national security risk.

Crucially, under DOJ's final rule, whether a transfer counts as **"bulk" depends on the data type** (e.g., much lower thresholds for biometric or precise geolocation data than for general identifiers), and counts are **aggregated over 12 months.** That makes **high-fidelity classification** non-negotiable.

Most organizations still don't know where sensitive data resides, who can access it, or how it moves across hybrid and multi-cloud environments. Cyera provides the visibility, intelligence, and automation CISOs need to operationalize EO 14117—turning compliance into a continuous, defensible security practice.

The Executive Order 14117 Mandate

EO 14117 ("Preventing Access to Americans' Bulk Sensitive Personal Data and U.S. Government-Related Data by Countries of Concern") imposes guardrails around:

- Transfers of U.S. persons' data to foreign entities.
- Visibility gaps into where sensitive or export-controlled data is stored and shared.
- Weak segmentation and controls in cloud and SaaS environments.

The rule sets **category-specific "bulk" thresholds** (e.g. **~1,000** for biometrics and precise geolocation; **~10,000** for health/financial data; **~100,000** for covered personal identifiers; special lower counts for human genomic/'omic data), with **12-month aggregation** across transactions.

Implications for CISOs

To meet these expectations, CISOs must:

- Identify which data qualifies as protected under national security or privacy risk categories, and which categories (e.g. biometric, geolocation, general personal identifiers) they belong to..
- Map and segment data by sensitivity, location, and jurisdictional exposure.
- Apply controls and prove ongoing due diligence with auditable evidence.

Because **"bulk" varies by category,** your program has to **apply the right threshold to the right data**—which demands **precise classification,** not broad labels.

Cyera: Data Intelligence for National Security–Grade Compliance

Cyera gives CISOs and their teams a real-time map of their data—where it lives, what it contains, and how it's accessed. Using advanced AI-driven classification and contextual analysis, Cyera helps you:

1. Identify and Classify Sensitive Data Automatically

- Discover structured and unstructured data across cloud, SaaS, and on-premises sources.
- Automatically identify data tied to U.S. persons, regulated categories, or export-controlled content.
- Go beyond regex: Classify data by context, owner, sensitivity, and EO 14117 category to determine which bulk threshold applies.

2. Segment and Protect High-Value Data

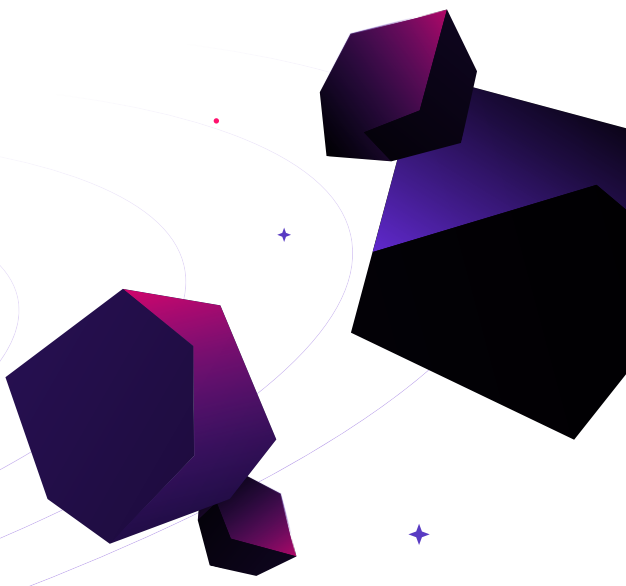
- Segment datasets by category and sensitivity, then apply data-aware policies that prevent copying/sharing to unapproved destinations or shadow tools.
- Detect and remediate cross-border exposure risks or foreign access pathways.
- Integrate with DLP, IAM, and SIEM solutions to enforce access and usage boundaries.

3. Govern AI Use

- **Discover** AI tools (including shadow AI) and monitor prompts/outputs/agent actions so regulated categories (e.g., health, financial, biometric) aren't fed to unapproved models.

4. Monitor and Report for Continuous Compliance

- Maintain an auditable record of where sensitive data resides and how it is secured.
- Automate reports to support federal compliance reviews and self-assessments.
- Visualize data lineage to demonstrate control and accountability across your environment.



How Cyera Accelerates EO 14117 Readiness

Challenge	Why it EO 14117 Expectation	Cyera's Solution
Limited visibility into data	Identify and protect U.S. persons' data	Unified data discovery across all environments
Cross-border data exposure	Prevent foreign access and misuse	Contextual location and access analysis
Fragmented controls	Enforce consistent segmentation	Policy-driven classification and control
Audit readiness gaps	Prove compliance and continuous monitoring	Automated reporting and dashboards

Outcome: From Reactive to Ready

Operationalizing EO 14117 with Cyera moves you from reactive risk mitigation to a proactive compliance posture that:

- Reduces exposure to regulatory and national security risk.
- Strengthens confidence in cloud and SaaS adoption.
- Demonstrates leadership in protecting your most sensitive digital assets.

Bottom line: Because **"bulk" is category-dependent,** accuracy matters. Cyera's combination of **DSPM precision, learned classifiers, data-aware controls, AI runtime governance,** and **continuous evidence** gives CISOs the exactitude needed to apply the **right thresholds to the right data**—and to prove it.


CYERA