PROGRAM MATERIALS
Program #36186
July 1, 2026

How to Comply with the Bulk Data Rule for Restricted Transactions

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 150, Boca Raton, FL 33487
Phone 561-241-1919

SLIDE 1

MISSION BRIEFING

BULK DATA RULE: TRANSACTIONS AND SECURITY REQUIREMENTS

Executive briefing on E.O. 14117, DOJ 28 CFR Part 202, and CISA security requirements

July 1
Celesq

Sources: CISA Security Requirements for Restricted Transactions (Jan. 2025); DOJ 28 CFR Part 202.

DISCLAIMER

The following presentation reflects the opinion of its human authors and does not necessarily represent the view of respective clients, partners, employers, or other of Amster, Rothstein & Ebenstein LLP, nor Celesq or any of its officers, or employees.

Additionally, the following content is presented solely for the purposes of discussion and illustration and does not comprise, nor is to be considered, as legal or business advice.

NO HUMANS WERE HURT IN MAKING THIS PRESENTATION, BUT AI ASSISTED IN ITS PREPARATION.

AI

No humans were hurt in making this presentation, but AI assisted in its preparation.

Celesq

ABOUT OUR SPEAKERS

CHARLES R. MACEDO

Charles R. Macedo is a seasoned intellectual property attorney with deep expertise at the intersection of emerging technologies, data-driven businesses, and commerce. He is recognized as an author, thought leader and frequent lecturer in intellectual property, blockchain, artificial intelligence/software, and data monetization. With a technical background in physics and decades of experience guiding Unicorns, startups, financial services firms, and technology innovators, he has developed IP strategies as they launch and monetize new product lines resulting in collections of hundreds of millions of dollars of royalty revenue.

J.D. 1989, Columbia Law School; B.S./M.S., Physics. 1986; former Law Clerk to Hon. Daniel M. Friedman at U.S. Court of Appeals for the Federal Circuit.

LEWIS DERENZIS III, M.S., J.D.

Lewis Derenzis III, M.S., J.D., is a Patent Agent and Law Clerk at Amster, Rothstein & Ebenstein LLP. Lewis brings valuable experience from his work as a Legal Intern at the SUNY Research Foundation, and at Alliant Cooperative Data Solutions.

J.D., Albany Law School, summa cum laude, Presidential Scholarship; M.S. Data Analytics, Western Governors University, B.S., Economics, magna cum laude, and Computer Science concentration, Iona College.

SLIDE 4

MISSION BRIEFING

TOPICS COVERED

- Overview of the Bulk Data Rule as it applies to restricted transactions
- Distinguishing prohibited vs. restricted transactions
- Required security controls under the Data Security Program
- The role of CISA security standards and guidance
- Practical compliance and documentation considerations

SLIDE 5

MISSION BRIEFING

LEARNING OBJECTIVES

After completing this program, participants will be able to:

1. Identify when a transaction qualifies as "restricted" under the Bulk Data Rule
2. Explain the security controls required for lawful restricted transactions
3. Evaluate common business arrangements for compliance risk
4. Advise clients on documenting and defending compliance in an enforcement environment

SLIDE 6

OVERVIEW OF THE BULK DATA RULE

DATA SECURITY PROGRAM

SLIDE 7

WHY THIS MATTERS

- National security rule — not just privacy
- Blocks foreign adversary access to sensitive U.S. data
- Targets cyber exploitation, AI training misuse, espionage

Sources: CISA Security Requirements for Restricted Transactions (Jan. 2025); DOJ 28 CFR Part 202.

SLIDE 8

REGULATORY ORIGIN

1 Feb. 28, 2024 — E.O. 14117

2 Jan. 3, 2025 — CISA Security Requirements

3 Jan. 8, 2025 — DOJ Final Rule (28 CFR Part 202)

Effective Apr. 8, 2025

Enforcement July 8, 2025

Full compliance Oct. 6, 2025

Sources: CISA Security Requirements for Restricted Transactions (Jan. 2025); DOJ 28 CFR Part 202.

SLIDE 9

WHAT THE RULE PROTECTS

1 Bulk U.S. sensitive personal data

2 Government-related data

3 Examples: health, financial, biometric, geolocation

4 Risk: access by countries of concern or covered persons

Sources: CISA Security Requirements for Restricted Transactions (Jan. 2025); DOJ 28 CFR Part 202.

SLIDE 10

WHO MUST CARE

1. U.S. persons engaging in covered data transactions
2. Legal and compliance teams
3. Cybersecurity and data governance leaders
4. Vendors, employers, and investors with data access

Sources: CISA Security Requirements for Restricted Transactions (Jan. 2025); DOJ 28 CFR Part 202.

SLIDE 11

KEY DEFINITIONS

KEY DEFINITIONS MAP

ACCESS

The ability to obtain or view data.

COVERED DATA TRANSACTION

A sale, transfer, or other transaction involving covered data.

COVERED PERSON

Person or entity linked to countries of concern.

COUNTRY OF CONCERN

Countries that pose a risk to U.S. national security.

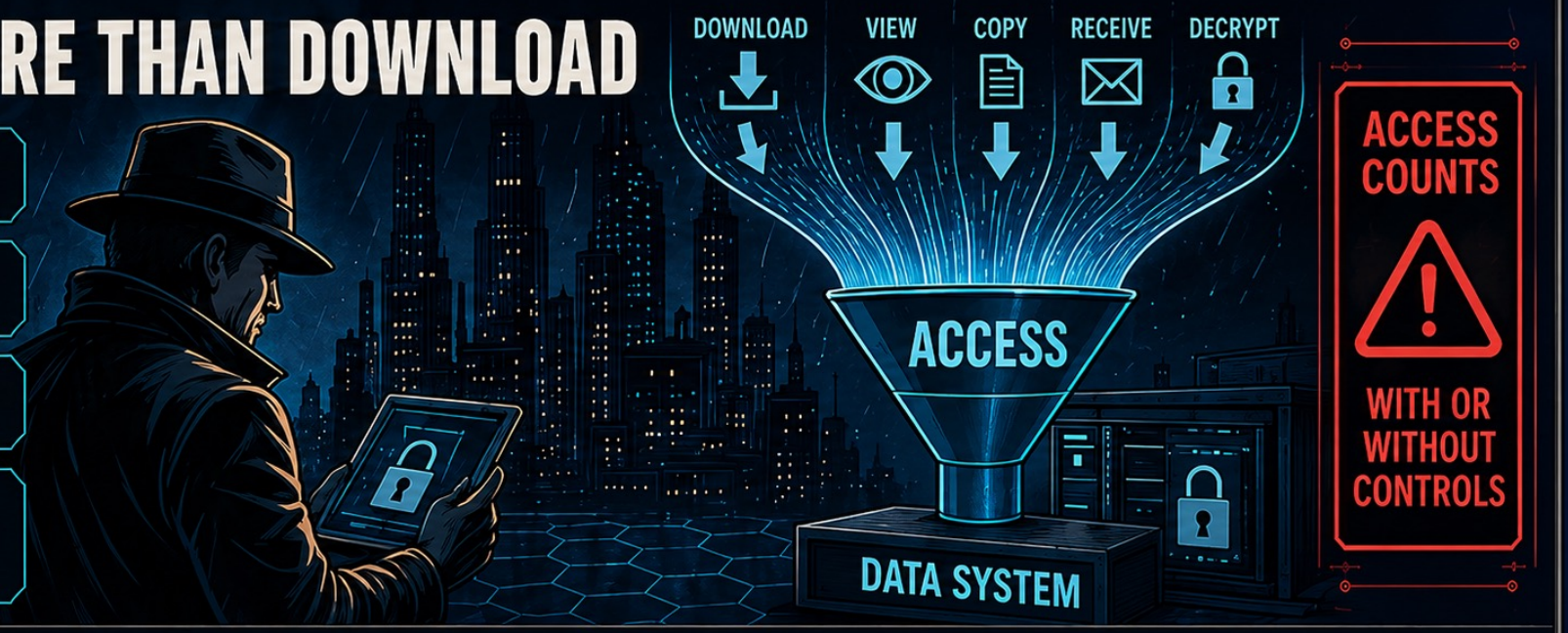
SECURITY REQUIREMENTS

Safeguards required to authorize and conduct transactions.

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

ACCESS MEANS MORE THAN DOWNLOAD

1. Obtain, read, copy, decrypt
2. Edit, release, alter, view, receive
3. Logical or physical access counts
4. Determine access without regard to security controls



Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 13

GOVERNMENT-RELATED DATA

1. Precise geolocation for listed sensitive U.S. locations — no bulk threshold
2. Sensitive personal data marketed as linked to current or recent former U.S. Government personnel
3. Military, intelligence, defense, law-enforcement, foreign-policy sensitivity

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 14

BULK U.S. SENSITIVE PERSONAL DATA

1. 
   Human omic data
2. 
   Biometric identifiers
3. 
   Precise geolocation
4. 
   Personal health
5. 
   Personal financial
6. 
   Covered personal identifiers
7. 
   Combined data

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 15

BULK THRESHOLDS

HUMAN GENOMIC	OTHER HUMAN OMIC / BIOSPECIMENS	BIOMETRIC	GEOLOCATION	HEALTH	FINANCIAL	COVERED PERSONAL IDENTIFIERS
						
>100 persons	>1,000	>1,000	>1,000	>10,000	>10,000	>100,000

COMBINED DATA

= LOWEST APPLICABLE THRESHOLD

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 16

COUNTRIES OF CONCERN

- CHINA (including Hong Kong and Macau)
- CUBA
- IRAN
- NORTH KOREA
- RUSSIA
- VENEZUELA

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 17

WHO IS A COVERED PERSON?

1. Covered entities owned 50%+ by countries of concern or covered persons
2. Entities organized or headquartered in a country of concern
3. Foreign individuals employed by covered entities or governments
4. Individuals primarily resident in a country of concern or specifically designated

COVERED PERSONS

- OWNERS
- EMPLOYEES
- RESIDENTS

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 18

COVERED DATA TRANSACTION

Any transaction involving access by a country of concern or covered person to government-related data or bulk U.S. sensitive personal data.

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 19

DECISION TREE: IS IT COVERED?

Is there government-related data or bulk U.S. sensitive personal data?

Is a country of concern or covered person getting access?

Does it involve data brokerage, vendor, employment, or investment agreement?

YES

NO

COVERED DATA TRANSACTION

EXEMPT / NOT COVERED

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 20

PROHIBITED VS. RESTRICTED

PROHIBITED =
CATEGORICALLY BANNED

EXAMPLES

- Data brokerage

VS.

RESTRICTED =
ALLOWED ONLY WITH COMPLIANCE MEASURES

EXAMPLES

- Vendor agreement
- Employment agreement
- Investment agreement

SECURITY REQUIREMENTS ARE DETERMINATIVE.

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 21

MISSION BRIEFING

PROHIBITED: DATA BROKERAGE

- Sale or license of data to recipient that did not collect it directly
- Government-related data or bulk U.S. sensitive personal data
- If recipient is a country of concern or covered person, the transaction is prohibited

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 22

MISSION BRIEFING

PROHIBITED: ONWARD TRANSFER RISK

- Onward transfer can still trigger prohibition
- Tracking pixels / SDKs can create prohibited data brokerage
- Know where the data ultimately goes

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 23

MISSION BRIEFING

PROHIBITED: HUMAN OMIC DATA AND BIOSPECIMENS

- Certain human omic data and biospecimen transactions are prohibited
- Rule is especially strict where access can enable sensitive exploitation
- Do not confuse research collaboration with permitted access unless a specific exemption applies

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 24

MISSION BRIEFING

RESTRICTED: VENDOR AGREEMENTS

- Third-party provider gets access to covered data
- Think hosting, IT support, analytics, cloud, processing
- Allowed only if rule conditions and CISA controls are satisfied

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 25

MISSION BRIEFING

RESTRICTED: EMPLOYMENT AGREEMENTS

- Employees, contractors, executives, directors
- Access — not title — drives the analysis
- Covered person access can make employment a restricted transaction

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 26

RESTRICTED: INVESTMENT AGREEMENTS

- Foreign ownership or rights in a U.S. entity or U.S. real estate
- Access to covered data is the risk
- Passive investment carve-outs may apply, but substantive rights can trigger restriction

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 27

TO PROCEED, SECURITY REQUIREMENTS ARE THRESHOLD

SECURITY CONTROLS

DUE DILIGENCE

No CISA-aligned controls = no authorized restricted transaction.

AUDITS

RECORDKEEPING

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.


REQUIRED SECURITY CONTROLS
DATA SECURITY PROGRAM
SECURE ACCESS
AUTHORIZED PERSONNEL ONLY
ACCESS STATUS
AUTHORIZED
MFA
VERIFIED
DEVICE HEALTH
COMPLIANT
ENCRYPTION
ACTIVE
SECURITY MONITORING
THREAT DETECTION
SYSTEM INTEGRITY
100%
SECURE
LOGS & EVENTS

SLIDE 29

CISA MODEL: TWO CONTROL TIERS

1 ORGANIZATIONAL- AND SYSTEM-LEVEL REQUIREMENTS

- **A.** ORGANIZATIONAL CONTROLS
- **B.** ACCESS
- **C.** RISK ASSESSMENT

2 DATA-LEVEL REQUIREMENTS

All layers work together to prevent access by covered persons and countries of concern.

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 30

WHAT IS A COVERED SYSTEM?

- An information system that interacts with covered data as part of a restricted transaction
- Includes systems that obtain, process, maintain, use, share, or dispose of the data
- Some workstations are excluded unless they interact with bulk data; government-related data has no bulk threshold

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 31

ORGANIZATIONAL CONTROLS

ORGANIZATIONAL CONTROL 1: ASSET INVENTORY

1. Identify, prioritize, and document covered-system assets
2. Maintain inventory with IP addresses where practicable
3. Update IT asset inventory at least monthly
4. Automated cloud inventory is acceptable

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 32

ORGANIZATIONAL CONTROLS

ORGANIZATIONAL CONTROL 2: LEADERSHIP ACCOUNTABILITY

1. Designate accountable cybersecurity leadership
2. Designate accountable governance, risk, and compliance leadership
3. May be one leader or separate owners

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 33

ORGANIZATIONAL CONTROLS

ORGANIZATIONAL CONTROL 3: KNOWN EXPLOITED VULNERABILITIES (KEV) REMEDIATION

1. Prioritize internet-facing covered systems
2. Remediate known exploited vulnerabilities within 45 calendar days
3. Use compensating controls if patching is not feasible
4. After patching, evaluate whether compromise occurred before remediation

ACTIONS

- IDENTIFY
- PRIORITIZE
- REMEDIATE
- VERIFY

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 34

ORGANIZATIONAL CONTROLS

ORGANIZATIONAL CONTROL 4: VENDOR/SUPPLIER DOCUMENTATION

1. Document and maintain all vendor and supplier agreements for covered systems
2. Include contractual IT and cybersecurity requirements
3. Think third-party network and service dependencies

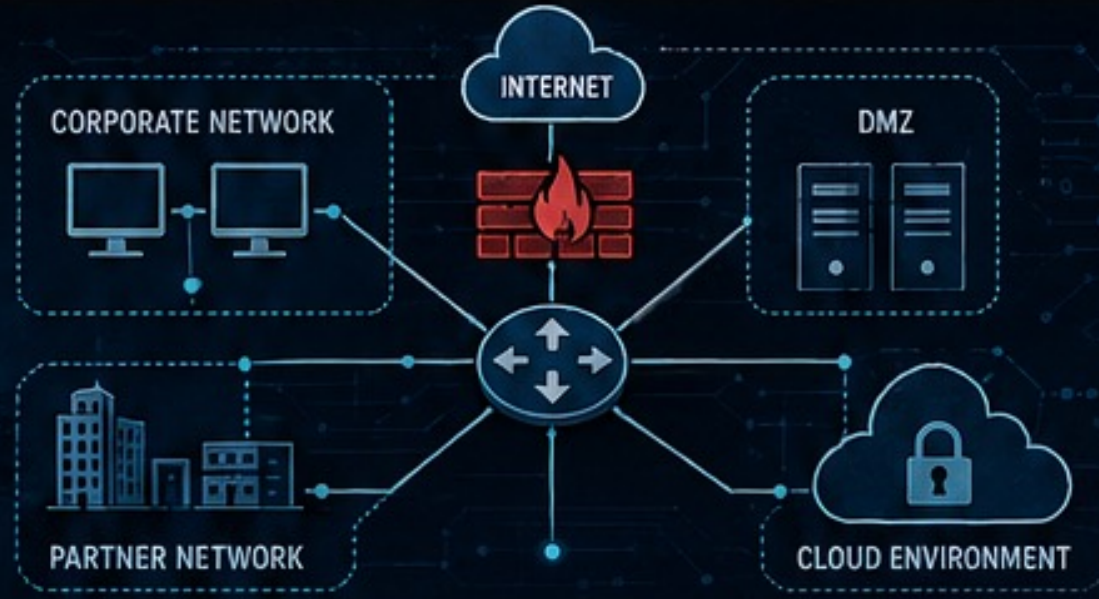
Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 35

ORGANIZATIONAL CONTROLS

ORGANIZATIONAL CONTROL 5: NETWORK TOPOLOGY

1. Maintain an accurate topology of the covered system
2. Map interfacing networks where technically feasible
3. Use it to improve visibility and incident response



Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 36

ORGANIZATIONAL CONTROL 6: APPROVALS AND ALLOWLISTS

1. Require approval before new hardware or software is deployed
2. Maintain a risk-informed allowlist of approved hardware and software
3. Control the attack surface before systems connect

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 37

ORGANIZATIONAL CONTROL 7: INCIDENT RESPONSE

1. Develop incident response plans for covered systems
2. Review annually and update as appropriate
3. Make plans usable for detection, response, and recovery

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 38

ACCESS CONTROL 1: MFA

1. Enforce multifactor authentication on all covered systems
2. Target strong authenticators such as AAL2 or AAL3
3. If MFA is not technically feasible, require passwords of 15+ characters

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 39

ACCESS CONTROL 2: REVOKE ACCESS FAST

1. Promptly revoke credentials and authorized access
2. Do so on departure or role change
3. Cover individual, shared, and system credentials

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 40

ACCESS CONTROL 3: LOGGING

1. Log access and security events
2. Monitor for critical log-source failure
3. Store logs centrally and securely
4. Retain for at least 12 months — longer if breach or violation remains unresolved

LOG-OURCE HEALTH

ALL SYSTEMS OPERATIONAL

CENTRAL LOG STORE

RETENTION

≥ 12 MONTHS

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 41

ACCESS CONTROL 4: DENY BY DEFAULT

- Configure covered systems and networks to deny all connections by default
- Require authentication or explicit allow rules
- Allow only specific functionality

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 42

ACCESS CONTROL 5: IDENTITY GOVERNANCE

- Issue and manage identities and credentials for users, services, and hardware
- Use attributes sufficient to block covered persons and countries of concern from impermissible access
- Limit access to authorized transactions and functions

BLOCK IMPERMISSIBLE ACCESS

- COVERED PERSONS
- COUNTRIES OF CONCERN

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 43

INTERNAL DATA RISK ASSESSMENT

- Evaluate whether selected controls truly prevent access
- Focus on linkable, identifiable, unencrypted, or decryptable data
- Assess likelihood of disclosure and harm
- Review annually and include a mitigation strategy

IMPACT	LIKELIHOOD: RARE	UNLIKELY	POSSIBLE	LIKELY	ALMOST CERTAIN
SEVERE	MEDIUM	HIGH	HIGH	CRITICAL	CRITICAL
MAJOR	LOW	MEDIUM	HIGH	HIGH	CRITICAL
MODERATE	LOW	MEDIUM	MEDIUM	HIGH	HIGH
MINOR	LOW	LOW	MEDIUM	MEDIUM	HIGH
NEGLIGIBLE	LOW	LOW	LOW	MEDIUM	MEDIUM

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

DATA LEVEL REQUIREMENTS

Source: CISA, Jan. 2025; DOI 28 CFR Part 202.

SLIDE 45

DATA MINIMIZATION AND MASKING

- Maintain a written retention and deletion policy
- Process data to reduce or eliminate covered status before access
- Techniques may include aggregation, pseudonymization, de-identification, anonymization
- Minimize linkability so identities cannot be inferred

COLLECT LESS. RETAIN LESS. REVEAL LESS.

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 46

ENCRYPTION AND KEY MANAGEMENT

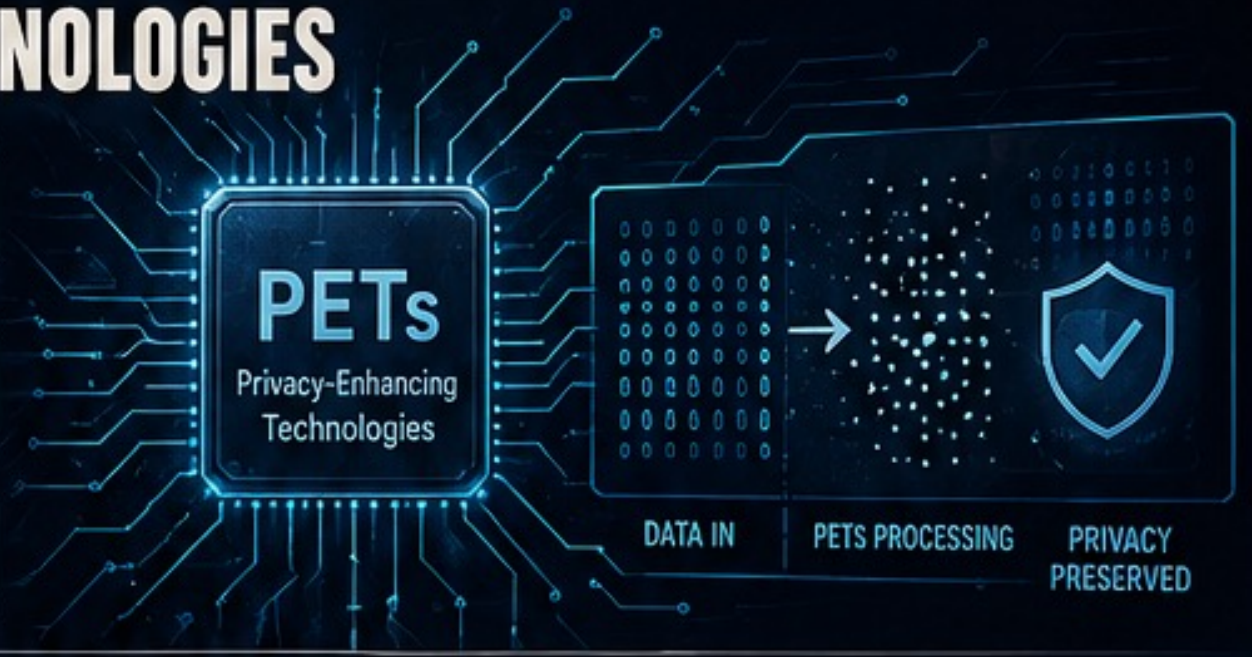
- Encrypt covered data in transit and at rest
- Use comprehensive encryption
- Do not co-locate keys with covered data
- Do not store keys in a country of concern or authorize covered persons to access them

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 47

PRIVACY-ENHANCING TECHNOLOGIES

- Use techniques such as privacy-preserving computation or differential privacy
- Processed data must not allow reconstruction of covered data
- Systems implementing these techniques are also covered systems



Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

PRACTICAL COMPLIANCE AND DOCUMENT CONSIDERATIONS

SLIDE 49

DUE DILIGENCE PROGRAM

- By Oct. 6, 2025, develop and implement a data compliance program
- Verify and log data types, volumes, parties, end use, and transfer method
- Use risk-based procedures for vendor identity checks
- Maintain written policies certified annually by a responsible officer

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

AUDIT REQUIREMENTS OVERVIEW

1 AUDIT REQUIRED

Annual audit required for any year the U.S. person engages in restricted transactions (on or after Oct. 6, 2025).

2 WHO MAY CONDUCT

- Qualified and competent
- Independent
- Cannot be a covered person or a country of concern.

3 WHEN & TIMEFRAME

- Once per calendar year in which restricted transactions occur
- Covers the preceding 12 months.

4 SCOPE

- Restricted transactions
- Data compliance program & implementation
- Relevant records
- Security requirements
- Reliable methodology

5 REPORT

- Written report within 60 days
- Include: nature of transactions, methodology & evidence, program effectiveness, vulnerabilities/deficiencies, control failures, recommendations.

6 RECORD RETENTION

Retain audit report for at least 10 years, consistent with recordkeeping requirements.

Source: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 51

RECORDKEEPING AND REPORTING

1. Keep full and accurate records of each covered transaction
2. Retain records for at least 10 years
3. Maintain annual certifications, due diligence evidence, and audit results
4. Be prepared for reports on demand, annual reports, and rejected prohibited transaction reports where applicable

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 52

PRACTICAL COMPLIANCE WORKFLOW

1. Know your data

2. Map transactions

3. Classify counterparty

4. Decide prohibited / restricted / exempt

- PROHIBITED
- RESTRICTED
- EXEMPT

5. Apply CISA controls

6. Update contracts

7. Monitor and audit

8. Retain evidence

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 53

EXECUTIVE KEY TAKEAWAYS

1. This is a national security regulation
2. Prohibited transactions are banned; restricted transactions require full compliance
3. Security requirements are determinative
4. Success requires legal, technical, and operational integration

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

SLIDE 54

RESTRICTED DOESN'T MEAN IMPOSSIBLE

IT MEANS CONTROLLED.

- KNOW THE DATA
- CONTROL THE ACCESS
- PROVE THE COMPLIANCE

Sources: CISA Jan. 2025; DOJ 28 CFR Part 202.

QUESTIONS?

We welcome your questions and discussion.

Celesq

Connect with Our Presenters

ARE LLP

CHARLES R. MACEDO

Lewis Derenzis III

Celesq