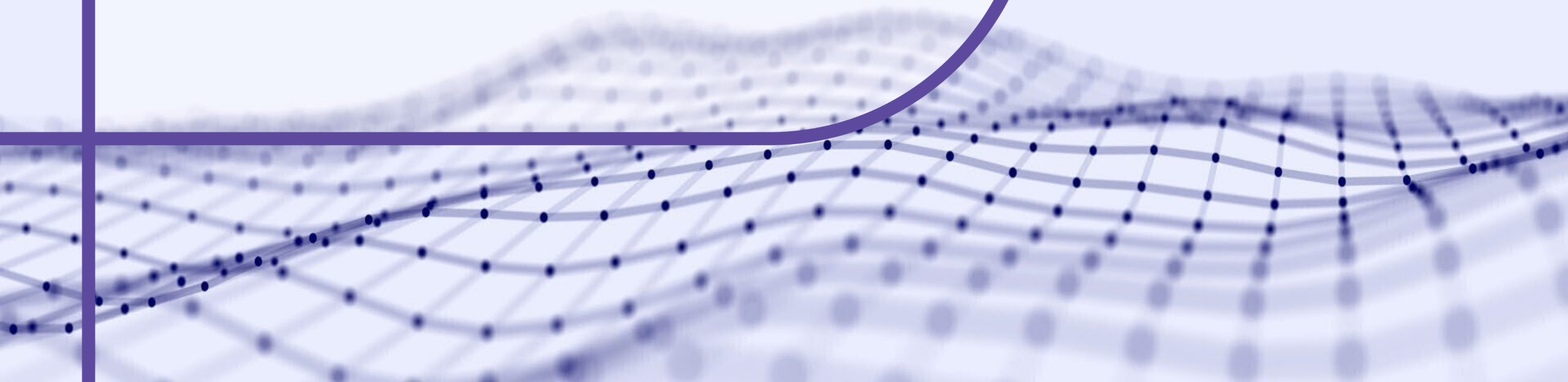
Perkins Coie

THE COMPLIANCE COLLECTIVE

DOJ's Data Security Program: Administrative, Audit, and Technical Requirements

MAY 21, 2026

SPEAKERS: DAVID AARON, SARAH GRANT, AND JOSH LAROCCA



The Compliance Collective

This webinar is a part of our monthly webinar series, “The Compliance Collective.”

The webinar series is hosted by a team of cross-disciplinary Perkins Coie lawyers who provide a monthly overview and discussion forum on a critical hot topic in ethics and compliance. Each topic provides a look at emerging issues and offers creative solutions to potential compliance problems.

The webinar is hosted every third Thursday at the same time each month: 10:00 a.m. PT/12:00 p.m. CT/1:00 p.m. ET.

Sign up on our website to receive invitations to our future webinars!

Agenda

- Overview of DOJ DSP
- Restricted Transactions
- Data Compliance Program
- CISA Requirements
- Audits
- Recordkeeping

David Aaron
SENIOR COUNSEL
Perkins Coie LLP
DAaron@perkinscoie.com

Sarah Grant
ASSOCIATE
Perkins Coie LLP
SarahGrant@perkinscoie.com

Josh Larocca
SENIOR MANAGING DIRECTOR
Stroz Friedberg
joshua.larocca@levelblue.com

DSP Overview

- 28 CFR Part 202
- Compliance requirements for “restricted transactions”
  - Due diligence
  - Technical safeguards
  - Data Compliance Program audits
  - Recordkeeping and reporting requirements

Restricted Transactions

- "Restricted transactions" = country of concern or covered person receives covered data or "access" to covered data through a vendor, employment, or investment agreement
- Permitted only if the U.S. person sharing data in those transactions complies with applicable requirements, including CISA security requirements

Data Compliance Program

- Vendor/employee/investor due diligence requirements
- Risk-based procedures
  - Verify data flows involved in any restricted transaction
  - Verify identities
- Written policies
  - Data compliance program
  - CISA security requirement
- Annual certification

CISA Requirements

- Purpose: mitigate risks associated with restricted transactions
  - Ensure that covered persons do not obtain actual access to covered data
- Begin with risk assessment
- Organization, system, and data levels
- Based on pre-existing standards
- Organizational & system-level requirements – all mandatory
- Data-level requirements – discretion to apply any combination that is effective to prevent covered persons' access
  - Based on risk assessment

Notes on CISA Requirements

- Compliance with CISA requirements does not mean the DSP does not apply

- Implementation of CISA requirements
  - May satisfy other cybersecurity requirements
  - Contributes to cybersecurity hygiene generally

Audits

- Establishing audit program
- Data mapping
- Comparison to other national security-oriented audit programs and privacy compliance programs
- Reasonableness
- Leveraging/combining with other audits

Recordkeeping and Reporting

- Retention periods
- Provision to DOJ upon request
- Self-reporting violations

CLE Code Word: Cybersecurity

Questions?

Perkins Coie