Quiz website: kahoot.it

ACC NCR: Protecting Data, Avoiding Liability: Navigating DOJ's Cybersecurity Initiatives

Townsend Bourne, Partner at Sheppard Mullin and ADG Co-Chair
Nikole Snyder, Senior Associate at Sheppard Mullin
Sherry Truong, Senior Privacy Counsel at Asana
Daniel Enos, In-House Counsel, Aerospace Defense and Technology

SheppardMullin

Pop Quiz! Test Question

Quiz website: kahoot.it

- What is your favorite Thanksgiving side dish?

DOJ Data Security Program

DOJ Data Security Program Rule – Background & Timeline

- Feb. 28, 2024 – Executive Order 14117, *Preventing Access to Americans' Bulk Sensitive Personal Data and U.S. Government-Related Data by Countries of Concern*
- Jan. 8, 2025 – Final Rule
- April 8, 2025 – Effective Date of Final Rule
- July 8, 2025 – 90-day grace period ends
- Oct. 6, 2025 – Deadline for compliance with all due diligence and audit provisions

DOJ Data Security Program

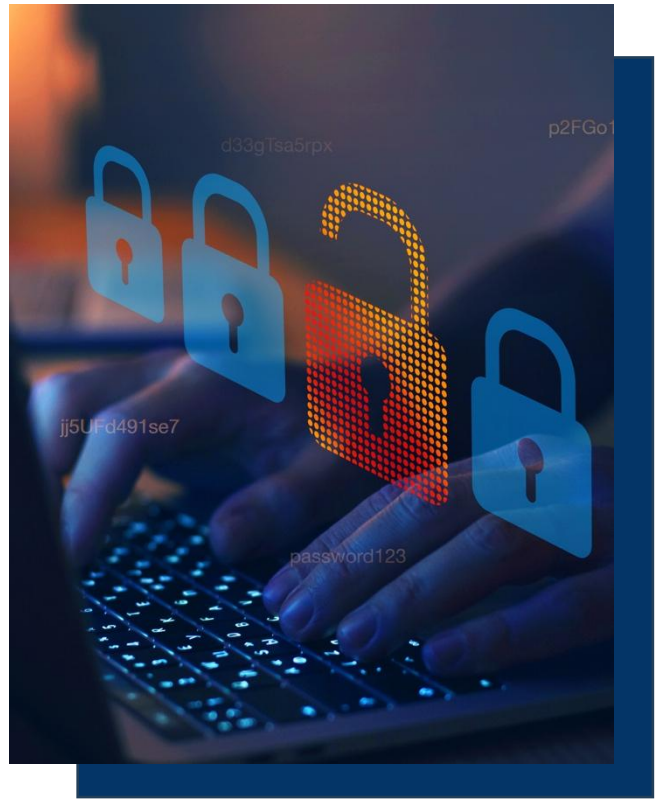
- The DOJ Data Security Program (DSP) prohibits or restricts "***covered data transactions***"
- Covered Data Transaction – *any* transaction that involves *any* access by a country of concern or covered person to *any* bulk U.S. sensitive personal data or government-related data and that involves data brokerage; a vendor agreement; an employment agreement; or an investment agreement. [28 CFR Part 202]

Two Types of Covered Data

- Bulk U.S. Sensitive Personal Data
- Government-Related Data

1. Bulk U.S. Sensitive Personal Data

- Bulk U.S. Sensitive Personal Data – a collection or set of sensitive personal data relating to U.S. persons, *in any format*, regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted, where such data meets or exceeds the applicable threshold.
- Bulk – any amount of sensitive personal data that meets or exceeds the thresholds *at any point in the preceding 12 months*, whether through a single covered data transaction or aggregated across covered data transactions involving the same U.S. person and the same foreign person or covered person.



Bulk Thresholds for Sensitive Personal Data

Sensitive Personal Data + Bulk Thresholds	
Data Types	**Bulk Threshold**
Human Genomic Data	100 U.S. Persons
Human ‘omic Data	1,000 U.S. Persons
Biometric Identifiers	1,000 U.S. Persons
Precise Geolocation Data	1,000 U.S. Devices
Personal Health Data	10,000 U.S. Persons
Personal Financial Data	10,000 U.S. Persons
Covered Personal Identifiers*	100,000 U.S. Persons

Covered Personal Identifiers

Covered Personal Identifiers
In combination or linked/linkable to other sensitive personal data
Gov’t ID / Account numbers (SSN, DL, Passport, etc.)
Financial Account numbers
Device-based Identifiers (IMEI, MAC, SIM)
Demographic / Contact Data (name, address, phone, email, etc.)
Advertising Identifiers (MAID, Google Ad ID, etc.)
Account-authentication Data (username, password, etc.)
Network-based Identifiers (IP address, cookie data)
Call-detail Data (CPNI)

Covered Personal Identifiers

- "Covered personal identifiers" *excludes*
  1. demographic or contact data that is linked only to other demographic or contact data; and
  2. a network-based identifier, account-authentication data, or call-detail data that is linked only to other network-based identifier, account-authentication data, or call detail data as necessary for telecommunications, networking, or similar service.

Pop Quiz! Question 1

Quiz website: kahoot.it

- A company has the following demographic data: first and last name linked to a residential street address, an email address linked to a first and last name, or a customer loyalty membership record linking a first and last name to a phone number.
- Is this a covered personal identifier?

Pop Quiz! Question 2

Quiz website: kahoot.it

- A U.S. company sells to a country of concern a list of residential addresses that the company describes as “addresses of members of a country of concern's opposition political party in New York City” or as “addresses of active-duty military officers who live in Howard County, Maryland” without any other listed identifiers or sensitive personal data.
- Is this a covered personal identifier?

2. Government-Related Data

- Government-Related Data – includes
  1. any precise geolocation data for any location on the Government-Related Location Data List (at § 202.1401) or
  2. any sensitive personal data marketed as linked or linkable to current or recent former employees or contractors, or former senior officials, of the U.S. Government.
- There is no bulk threshold for Government-related data, so any single data point is considered covered data.

Country of Concern or Covered Persons

- Countries of Concern – China, Cuba, Iran, North Korea, Russia, and Venezuela
- Covered Person – a foreign person as set forth below or any person on the DOJ National Security Division (NSD) Covered Persons List:
  - (1) Entity 50% or more owned, directly or indirectly, by one or more countries of concern or persons described in (2); or organized or chartered under the laws of, or has its principal place of business in, a country of concern;
  - (2) Entity 50% or more owned, directly or indirectly, by one or more persons described in (1), (3), (4), or on the NSD Covered Persons List;
  - (3) An individual who is an employee or contractor of a country of concern or entity described in (1), (2), or on the NSD Covered Persons List; or
  - (4) An individual who is primarily a resident in the territorial jurisdiction of a country of concern.

Pop Quiz! Question 3

Quiz website: kahoot.it

- A foreign person is located abroad and is employed by a company headquartered in China.
- Is this a covered person?

Pop Quiz! Question 4

Quiz website: kahoot.it

- Chinese or Russian citizens located in the United States.
- Is this a covered person?

Country of Concern or Covered Persons

- Foreign Person – any person that is not a U.S. person.
- U.S. Person – any U.S. citizen, national, or lawful permanent resident; any refugee under 8 U.S.C. 1157 or asylee under 8 U.S.C. 1158; any entity organized solely under U.S. law (including foreign branches); ***or any person in the United States***.

Prohibited and Restricted Transactions

Prohibited Transactions

- Prohibition – No U.S. person may knowingly engage in a covered data transaction involving data brokerage with a country of concern or covered person.
  - Data brokerage – the sale of data, licensing of access to data, or similar commercial transactions, excluding an employment agreement, investment agreement, or vendor agreement, involving the transfer of data from any person to any other person, where the recipient did not collect or process the data directly from the individuals linked or linkable to the collected or processed data.
  - A transaction does not necessarily need to involve monetary value or valuable consideration exchanged. The relevant consideration is whether a transaction enables access to covered data.
- Covered data transactions with countries of concern or covered persons involving access to bulk human 'omic data, or to human biospecimens from which bulk human 'omic data could be derived are also prohibited.

Data brokerage transactions with Foreign Persons

- Where a U.S. person knowingly engages in a data brokerage transaction with any foreign person that is not a covered person involving any access by a foreign person to government-related data or bulk U.S. sensitive personal data, the U.S. person must
  1. contractually require the foreign person to refrain from engaging in a subsequence covered data transaction involving data brokerage of the same data with a country of concern or covered person; and
  2. report any known or suspected violation of the contractual requirement.

Compliance Obligations

- Cease any data brokerage transactions that are prohibited transactions with a country of concern or covered person.
- Institute contractual requirements in data brokerage agreements with foreign persons.
  - Take reasonable steps to evaluate compliance by foreign persons, such as conducting due diligence as part of a risk-based compliance program and requiring periodic certifications of compliance.
  - Report known or suspected violations of contractual requirements within 14 days.
- Report instances where the Company rejects participating in a prohibited transaction involving data brokerage within 14 days of the rejection.

Restricted Transactions

- Restriction – No U.S. person may knowingly engage in a covered data transaction involving a vendor agreement, employment agreement, or investment agreement with a country of concern or covered person unless the U.S. Person complies with the CISA Security Requirements and other applicable requirements.

Pop Quiz! Question 5

Quiz website: kahoot.it

- A U.S. business knowingly enters into an agreement to buy bulk human genomic data from a European business that is not a covered person.
- Is this a prohibited transaction?

Pop Quiz! Question 6

Quiz website: kahoot.it

- A U.S. company engages in an employment agreement with a covered person to provide information technology support. As part of their employment, the covered person has access to personal financial data. The U.S. company implements and complies with the security requirements.
- Is this a restricted transaction? Is it authorized?

Compliance Obligations for Restricted Transactions

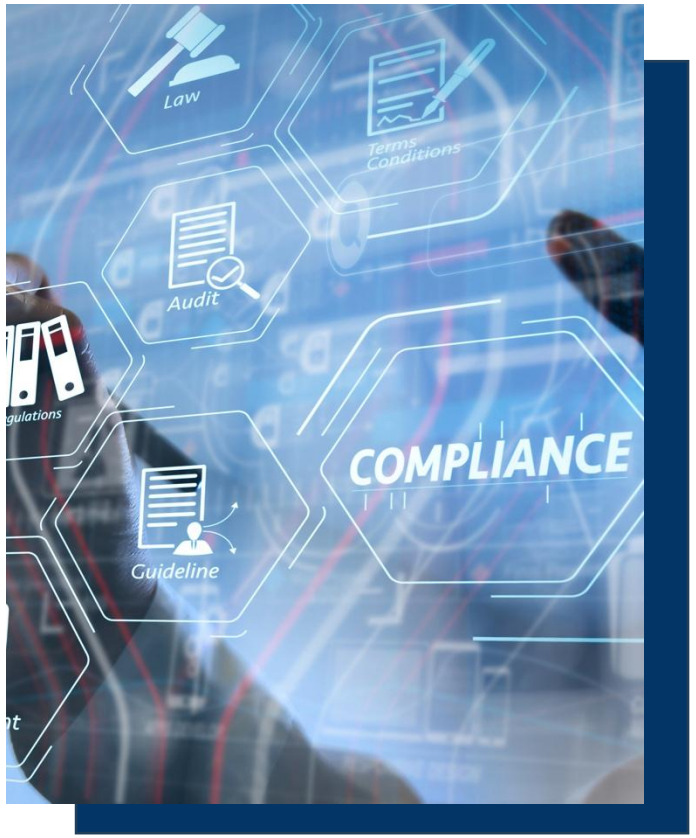
1. Implement CISA Security Requirements – The goal of these requirements is to prevent a covered person and/or country of concern from accessing covered data.
   - There are two categories of security requirements:
     1. Organizational- and system-level, and
     2. Data-level

Compliance Obligations for Restricted Transactions

2. Develop, implement, and routinely update the Company's Data Compliance Program to include:
   - Risk-based procedures
     - Verify and log, in an auditable manner: (i) types and volumes of covered data involved in any restricted transactions; (ii) identity of transaction parties, including any ownership of entities or citizenship or primary residence of individuals; and (iii) end-use of data and the method of data transfer.
     - Consider annual risk assessment that examines: (i) current security measures; (ii) vendors, investors, and employees; (iii) offered products and services; (iv) coverages under existing general or specific licenses or exemptions; and (v) geographic locations of the Company, including vendors, subsidiaries, affiliates, etc. Also consider risk assessment for mergers/acquisitions or other corporate transactions.
     - Internal controls, including written policies and procedures. Consider procedure for bringing newly acquired entities into compliance.

Compliance Obligations for Restricted Transactions

- Vendor management and validation to include screening vendors to verify whether they are covered persons.
  - Consider screening software that (i) reviews and incorporates updates to the Covered Persons List and other relevant U.S. government lists; (ii) accounts for identifiers and alternative spellings; (iii) accounts for organizational hierarchy; (iv) considers vendors' geographic location; and (v) screens against current, newly added, and prospective vendors.
- Written policy describing the Data Compliance Program that is annually certified by an officer, executive, or other employee responsible for compliance.
  - Communicate and confirm understanding of the policy with relevant personnel.
  - Conduct annual review and certification of written policies and procedures.



Compliance Obligations for Restricted Transactions

- Written policy describing implementation of the CISA Security Requirements that is annually certified by an officer, executive, or other employee responsible for compliance.
- Consider annual training on the Data Compliance Program and CISA Security Requirements for all relevant employees and personnel.
- Appoint a Compliance manager with senior-level authority, sufficient technical expertise, and resource support to implement Data Compliance Program. Ensure senior manager support and buy-in.

Compliance Obligations for Restricted Transactions

3. Audit annually the Company's data transactions; Data Compliance Program; compliance with CISA Security Requirements; all related software, systems, and other technology; and relevant records. Within 60 days of audit completion, submit a report on findings to a senior officer of the Company. Retain audit reports for at least 10 years.

Compliance Obligations for Restricted Transactions

4. Recordkeeping and Reporting
   - The Company must keep full and accurate records of each transaction subject to the DSP. Retain records for at least 10 years. Additional recordkeeping requirements as described above, and senior official must sign annual certification of completeness and accuracy of the Company's recordkeeping, as supported by an audit.
   - Provide reports from time to time as may be required by NSD.
     - Annual reporting requirement for any U.S. person that:
       - Engages in a restricted transaction involving cloud-computing services, and
       - That has 25% or more of the U.S. person's equity interests owned (directly or indirectly) by a country of concern or covered person.

Exemptions

Exemptions

Communication

Postal, telegraphic, telephonic, or other personal communication that does not involve the transfer of anything of value is exempted.

Routine Financial Services

Data transactions are exempted (i.e., neither prohibited nor restricted) if they are ordinarily incident to and part of the provision of financial services. This includes transfer of personal financial data or covered personal identifiers incidental to the purchase and sale of goods and services (such as purchase of consumer products and services through online shopping or e-commerce marketplaces).

Exemptions

Corporate Group Transactions

Transactions are exempted (i.e., neither prohibited nor restricted) if they are (1) between a U.S. company and its subsidiary or affiliate in a country of concern, and (2) ordinarily incident to and part of administrative or ancillary business operations.

Telecommunications

Data transactions ordinarily incident to and part of the provision of telecommunications services, including international calling, mobile voice, and data roaming are exempted.

Licenses

Licenses

- NSD may grant a license to authorize transactions that would otherwise be prohibited or restricted. Note we expect licenses will be authorized only in limited circumstances and it should not be assumed the Company will be granted a license.
- There are two types of licenses:
  - General
  - Specific

Licenses

- General License – a written license authorizing a class of transactions and not limited to a particular person.
  - All general licenses will be published on the NSD website and in the Federal Register. General licenses are self-executing and do not require or allow applications.
- Specific License – a written license issued to a particular person or persons, authorizing a particular transaction or transactions in response to a written license application.
  - Applications for specific licenses must be submitted via email to NSD.FIRS.datasecurity@usdoj.gov or via electronic means on the NSD website. Applications shall include a description of the nature of the transaction. Refer to § 202.802 for the full application requirements.

Enforcement & Penalties

Enforcement and Penalties

- NSD may bring civil enforcement actions and criminal prosecutions for knowing or willful violations of DSP requirements.
- Unlawful acts are subject to civil penalties of up to the greater of $368,136 or twice the value of each violative transaction.
- Willful violations are punishable by imprisonment of up to 20 years and a $1,000,000 fine.

False Claims Act & DOJ Civil Cyber Fraud Initiative

Pop Quiz! Question 7

Quiz website: kahoot.it

- Which of the following actions could trigger DOJ investigation under the Civil Cyber-Fraud Initiative?

  A. Data breach disclosure

  B. Failure to follow required security controls

  C. Knowingly falsifying compliance documents

  D. All of the above

False Claims Act (Refresher)

- **False Claims Act Elements:**
  - Claim for payment (e.g., invoice)
  - Falsity (objectively false)
  - Knowledge (actual, deliberate indifference, reckless disregard)
  - Materiality (violation, if known to the USG, would *actually influence* its payment decision)
- **Potential FCA Penalties:**
  - Per claim penalties from $13,508 to $27,018 USD
  - Treble (3x) damages
  - Relator's attorneys' fees

DOJ Civil Cyber Fraud Initiative (CCFI)

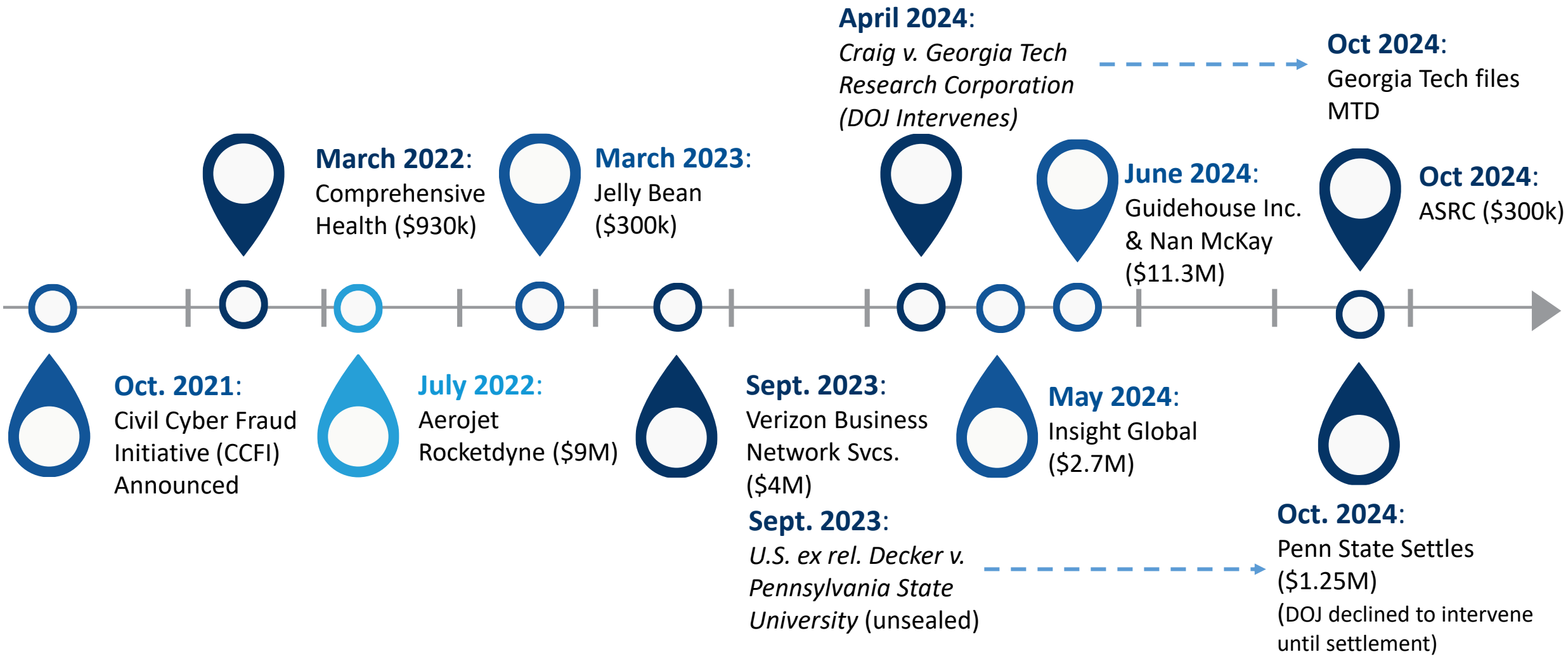
- In **October 2021**, the US Department of Justice announced a new Civil Cyber Fraud Initiative to use the False Claims Act to enforce cybersecurity standards and reporting requirements
- **Announced Purpose:**
  - Holding contractors and grantees to their commitments to protect government information and infrastructure.
  - Supporting government experts' efforts to timely identify, create and publicize patches for vulnerabilities in commonly-used information technology products and services.
  - Ensuring that companies that follow the rules and invest in meeting cybersecurity requirements are not at a competitive disadvantage.
  - Reimbursing the government and the taxpayers for the losses incurred when companies fail to satisfy their cybersecurity obligations.
  - Improving overall cybersecurity practices that will benefit the government, private users and the American public.

Pop Quiz! Question 8

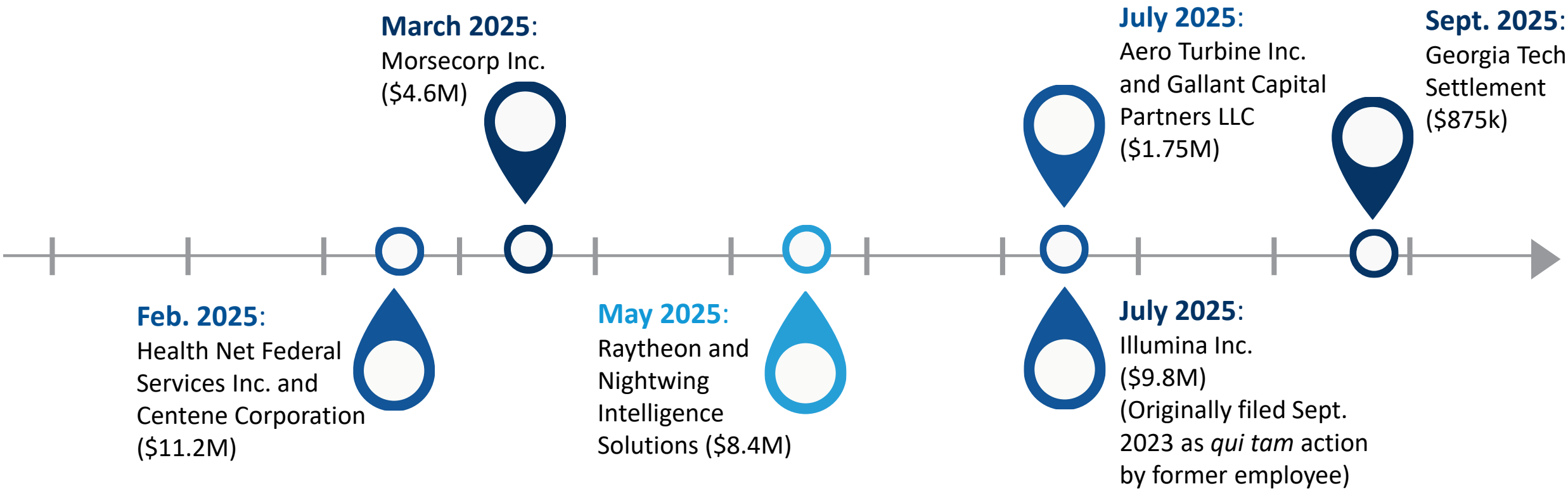
Quiz website: kahoot.it

- Contractors can only be held liable under the initiative if a cyber incident or breach actually occurs.
- True or false?

Timeline: Civil Cyber Fraud Initiative FCA Actions – History



Timeline: Civil Cyber Fraud Initiative FCA Actions – 2025 Developments



Pop Quiz! Question 9

Quiz website: kahoot.it

- True or False: Only federal defense contractors are subject to FCA cyber fraud enforcement.
- True or false?

Case Studies: Recent Cyber FCA Cases

Case Study: ATI and Gallant (July 2025)

Overview

- Cybersecurity requirements stem from an ATI contract with the Air Force
- ATI submitted two written disclosures
- Both ATI and Gallant cooperated fully and took remedial measures
- Settlement of $1.75m resolves liability for:
  - (1) Failure to implement NIST SP 800-171 cybersecurity controls as required by DFARS 252.204-7012 from January 2018 to February 2020
  - (2) Failure to control flow of and access to CUI from June 2019 to July 2019
- The settlement credited ATI and Gallant for disclosure, cooperation, and remediation actions, resulting in a multiplier of ~1.5x

Case Study: ATI and Gallant

Takeaways

- Private Equity as an FCA Hook
  - Gallant was liable in the FCA settlement as a private equity company for owning a controlling stake of ATI "through investment funds for which it acted as an advisor"
  - This development puts private equity firms on notice that a controlling stake in companies may be sufficient for FCA liability
- Increased Scrutiny for Sensitive Information
  - Entities that handle private and sensitive information, such as medical records, genomic data, or CUI should pay particular attention to cybersecurity requirements
- Cooperation Pays Off
  - Cooperation credit provides significant financial motivation for contractors to disclose/cooperate

Pop Quiz! Question 10

Quiz website: kahoot.it

- A company can face FCA liability for misrepresenting its compliance with federal cybersecurity requirements in government contract bids.
- True or False?

Raytheon and Nightwing Group Settlement (May 2025)

- Settlement of $8.4m for allegations of non-compliance with cybersecurity requirements in DoD contracts
  - Whistleblower recovery – $1.512m (former Raytheon Director of Engineering)
- Allegations include:
  - Failed to develop and implement a system security plan
  - Failed to ensure that the system complied with DFARS 252.204-7012
  - Failed to ensure that the system complied with FAR 52.204-21
  - Used noncompliant internal system to develop, use, or store CDI and FCI during its performance on 29 DoD contracts and subcontracts.
- Nightwing acquired Raytheon Cybersecurity, Intelligence, and Services business in March 2024

Case Study: *U.S. ex rel. Decker v. Pennsylvania State University*

- Settlement of $1.25M (October 2024)
  - Case initially brought by whistleblower (former CIO of Penn State's Applied Research Lab)
- DOJ alleged Penn State violated contractual requirements to:
  - Submit the date by which it expected all NIST security controls to be implemented (i.e., a score of 110) per DFARS 252.204-7019 & -7020
  - Adequately document its plan to implement the security controls
  - Utilize external cloud service providers that meet the security requirements in the FedRAMP Moderate baseline per DFARS 252.204-7012(b)(2)(ii)(D))
- Related to 15 contracts/subcontracts from 2018-2023

Case Study: *U.S. ex rel. Decker v. Pennsylvania State University*
Key Takeaways

Almost all agreements were subcontracts supporting DoD (*i.e.*, Penn State not the prime)	Reminder the cyber requirements apply to *all* contractors (direct or indirect).
Misrepresentation relating to POA&M dates (not overall cyber score)	Demonstrates the breadth of DOJ's focus (*i.e.*, *all* requirements).
Currently, no POA&M timeline (will change with CMMC)	Reminder to be mindful of *any* representation made to the USG.
No incident or breach, low settlement amount, and no mention of restitution	May indicate difficulty showing actual damages.

Case Study: *Craig v. Georgia Tech Research Corporation*

Overview

- Whistleblower suit (July 2022)
  - Initiated by former senior members of Georgia Tech's Cybersecurity team
- DOJ intervention, unsealed (Feb. 2024)
- DOJ Complaint is 99 pages (quite detailed)
- Failure to comply with DFARS -7012, -7019, -7020; FAR 52.204-21
- Claims: False Claims Act and federal common law (including fraud, negligent misrepresentation, breach of contract, unjust enrichment, and payment by mistake)
- $19M in payments resulting from allegedly false invoices
- $875k settlement (Sept. 2025)

Case Study: *Craig v. Georgia Tech Research Corporation*

GTRC's Motion to Dismiss

> The government's own inability to untangle this complex and evolving contractual and regulatory scheme demonstrates why the government cannot plead its claims at all, much less under the heightened Rule 9(b) pleading standard applicable here.

Case Study: *Craig v. Georgia Tech Research Corporation*

DOJ's Complaint (Key Allegations)

- Failure to provide "adequate security" including failure to:
  - develop and implement a system security plan (SSP) to implement security controls from NIST SP 800-171
  - install, update or run anti-virus or anti-malware tools on IT equipment at the lab
- Even after implementing an SSP, failure to properly scope that plan to include all covered equipment (i.e., laptops, desktops, and servers).
- Submission of a false cybersecurity assessment score to DoD for the Georgia Tech campus.
  - DOJ alleges the submission of a score was a "condition of contract" award and Georgia Tech and GTRC submitted a false score of 98 (a perfect score is 110).

GTRC's Motion to Dismiss (Key Defenses)

- The DoD cybersecurity regulations do not apply to systems used to perform fundamental research (*i.e.*, no CDI).
- Strict compliance with the cybersecurity controls was not material
  - Contracting officer never considered/relied on GTRC's compliance or verified the SPRS score
  - No minimum SPRS score demonstrates the score is immaterial
- The certifications submitted with invoices did not mention cybersecurity rules nor certify compliance with them.
- There was no harm to the Government (no allegation any information was compromised).

Lessons

FCA Risks

- Accepting clauses that do not apply
- Making representations to “check the box”
- Assuming subcontractors are insulated from risk
- Failing to adopt required cybersecurity standards
- Misrepresenting cybersecurity compliance
- Failing to report incidents or breaches

Risk Mitigation

- Attempt to reject inapplicable clauses/ get clarity from the KO
- Document compliance efforts
  - Including “gray areas”
- Be transparent
- Consider voluntary disclosure / full cooperation

Questions?

Pop Quiz! Question 11

Quiz website: kahoot.it

- A U.S. company advertises the sale of a set of sensitive personal data as belonging to “active duty” personnel, “military personnel who like to read,” “DoD” personnel, “government employees,” or “communities that are heavily connected to a nearby military base.”
- Is this government-related data?

Pop Quiz! Question 12

Quiz website: kahoot.it

- Foreign persons primarily resident in Cuba.
- Is this a covered person?

Pop Quiz! Question 13

Quiz website: kahoot.it

- A U.S. person engages in a vendor agreement with a covered person involving access to bulk U.S. sensitive personal data. The vendor agreement is a restricted transaction. To comply with the CISA security requirements, the U.S. person, among other things, uses data-level requirements to mitigate the risk that the covered person could access the data.
- Is the vendor agreement a covered data transaction?

Pop Quiz! Question 14

Quiz website: kahoot.it

- A covered person engages in a vendor agreement with a U.S. person involving the U.S. person accessing bulk U.S. sensitive personal data already possessed by the covered person.
- Is this a covered data transaction?

Pop Quiz! Question 15

Quiz website: kahoot.it

- A U.S. company engages in a vendor agreement with a covered person to store bulk personal health data. Instead of implementing the security requirements as identified by reference in this subpart D, the U.S. company implements different controls that it believes mitigate the covered person's access to the bulk personal health data.
- Is this a restricted transaction? Is it authorized?