Life Sciences Trends & Topics
WEBCAST SERIES

Fortifying Cybersecurity in Life Sciences

A COMPREHENSIVE APPROACH

MARCH 19, 2025

Welcome

BRAD STEWART
Market Managing Principal
Life Sciences National Leader

brad.stewart@bdo.com

With You Today

ERIC CHUANG
Cybersecurity
Managing Director

echuang@bdo.com

CLYDE HARRIS
Industry Specialty Services
Senior Manager

charris@bdo.com

JAMES NEAL
Principal & NetSuite
Practice Lead

jneal@bdo.com

Learning Objectives

Upon completion of this session, participants will be able to:

- Discuss the critical importance of compliance with data protection regulations & how to navigate the complex regulatory environment effectively
- Discover the key components of a comprehensive privacy control & reporting framework that caters to the unique needs of the life sciences industry
- Review practical strategies & best practices to enhance your company's cybersecurity posture, mitigate risks & protect sensitive data
- Discuss the importance of staying ahead in cybersecurity efforts to safeguard your company's future in an ever-evolving digital landscape

Agenda

Cybersecurity Threats Specific to Life Sciences

Overview of Department of Defense (DoD) Requirements Linked to IT systems

Life Sciences Industry Requirements

Q&A

Life Sciences Trends & Topics
WEBCAST SERIES

Cybersecurity Threats Specific to Life Sciences

Adversaries Specifically Targeting Life Sciences Industry

Criminal Enterprises

Insiders

Nation States

Criminal Enterprises

Financially Motivated

- Low effort - Capitalize on weaker links in a diverse industry
- High Payout – Higher likelihood of sensitive data

Methodology

- Traditional tools and tactics

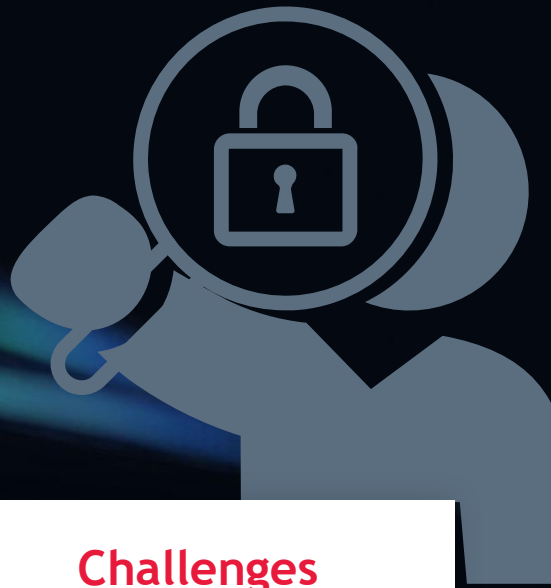
Mitigation

- Defendable with IT/Cyber security

Challenges

- High Volume and continuous
- Overhead vs. profit
- Fatigue and complacency
- False sense of security

Insiders



Financially Motivated

- Self-interest
- 3rd-party

Methodology

- Traditional vs. digital
- Recruitment
- Theft vs. sabotage

Mitigation

- Personnel focused
- Access focused

Challenges

- Credentialed access
- Business culture - compartmentalization
- Employee privacy - vetting
- Lack subject matter expertise

Nation State

IP and National Interest Motivated

Methodology

- Zero-days
- Infrastructure
- Vendor
- Supply Chain
- IoT

Mitigation

- Standard IT/Cyber security insufficient

Risks

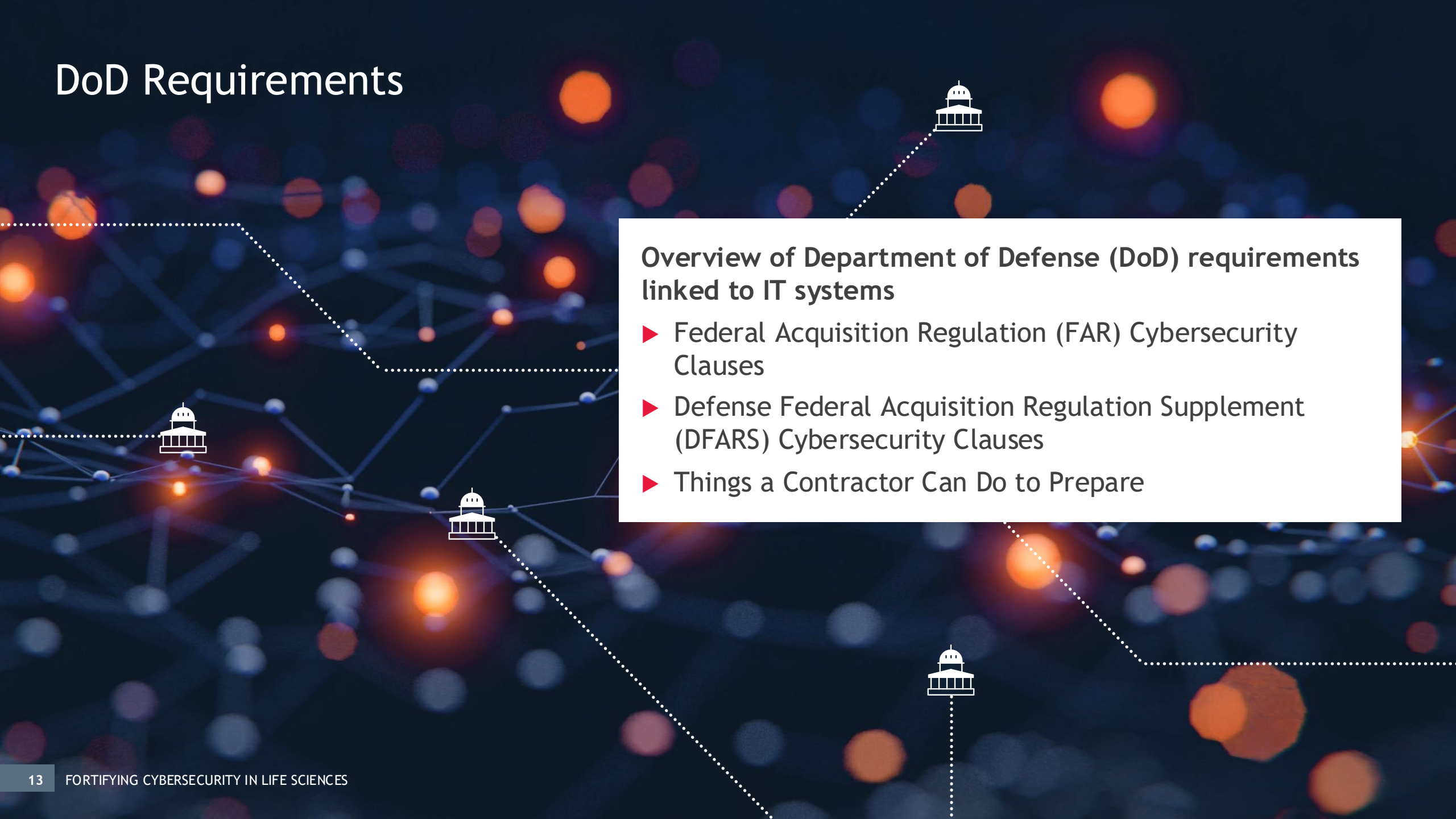
- Tools and methodology yet undefendable - Zero Days
- Unprotected equipment
- Lack subject matter expertise
- Business culture change

Life Sciences Trends & Topics
WEBCAST SERIES

Overview of Department of Defense (DoD) Requirements Linked to IT systems

BDO

DoD Requirements



Overview of Department of Defense (DoD) requirements linked to IT systems

- Federal Acquisition Regulation (FAR) Cybersecurity Clauses
- Defense Federal Acquisition Regulation Supplement (DFARS) Cybersecurity Clauses
- Things a Contractor Can Do to Prepare

Federal Acquisition Regulation (FAR)

CYBERSECURITY CLAUSES

- **FAR 52.204-XX - New Proposed CUI Rule**
- **FAR 52.204-YY - New FAR Proposed [No CUI] Rule**
- **FAR 52.204-21** - Basic Safeguarding of Covered Contractor Information Systems
- **FAR 52.204-23** - Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab
- **FAR 52.204-25** - Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (Section 889)
- **FAR 52.204-26** - Covered Telecommunications Equipment or Services—Representation
- **FAR 52.204-27** - TikTok Prohibition
- **FAR 52.239-1** Privacy or Security Safeguards

Standalone Agency CUI Clauses

Department of Energy:

- **DOE Order 471.7** - Controlled Unclassified Information

Department of Homeland Security:

- **HSAR 3052.204-72**: Safeguarding of Controlled Unclassified Information

Department of Defense (DoD)

CYBERSECURITY CLAUSES

- **DFARS 252.204-7008** - Compliance with Safeguarding Covered Defense Information Controls
- **DFARS 252.204-7009** - Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information
- **DFARS 252.204-7012** - Safeguarding Covered Defense Information and Cyber Incident Reporting
- **DFARS 252.204-7018** - Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services
- **DFARS 252.204-7019** - Notice of NIST SP 800-171 DoD Assessment Requirements
- **DFARS 252.204-7020** - NIST SP 800-171 DoD Assessment Requirements
- **DFARS 252.204-7021** - Cybersecurity Maturity Model Certification (CMMC) Requirements *New in rulemaking 48 CFR
- **DFARS 252.204-7024** - Notice on the Use of the Supplier Performance Risk System
- **DFARS 252.225-7048** - Export-Controlled Items
  - **Export Administration Regulations (EAR)** - Controls the export of dual-use and commercial items.
  - **International Traffic in Arms Regulations (ITAR)** - Controls the export and import of defense-related articles and services.
- **DFARS 252.239-7010** - Cloud Computing Services
- **DFARS 252.239-7016** - Telecommunications Security Equipment, Devices, Techniques, and Services

FAR CLAUSE - FAR 52.204-21

Understanding “Basic Cyber Hygiene”

FAR 52.204-21:
Basic Safeguarding of Covered Contractor Information Systems

Defines FCI

Information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

Safeguarding

Requires application of basic safeguarding requirements when processing, storing, or transmitting Federal Contract Information (FCI) in or from covered contractor information systems.

- Defines **“Basic Cyber Hygiene”**
- 15 Security Controls to Implement
- Mandatory Flow-down to Subcontractors

DFARS 252.204-7012

Safeguarding for Controlled Unclassified Information (CUI)

DFARS 252.204-7012:
Safeguarding Covered Defense Information and Cyber Incident Reporting

Defines CUI

Information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government.

NARA archives: Classification for CUI Categories
https://www.archives.gov/cui/registry/category-list

Exemption: Manufacturers of COTS / Commercial Items

Provide "Adequate Security"
NIST SP 800-171

System Security Plan (SSP)
requirements **to be implemented**

Plan of Action and Milestones (POA&M)
requirements **not yet implemented**

Mandatory Flowdown Clause to Subcontractors

Safeguard Covered Defense Information (CDI)
(read: CUI)

Report Cyber Incidents within 72 hours: DIBNET
DoD Cyber Crime Center (DC3)

Report Malicious SW
Facilitate Damage Assessment

Things a Contractor Can Do to Prepare for CUI Clauses

Scoping

- Know what clauses are in your current contracts
- Look ahead - Know what the agencies you **want to contract with** may have for CUI clauses before you bid
- Know what CUI you have on your systems currently and where those files are stored and shared
- Know who in your organization has access to these files
- Know what systems you store them on – not all systems are compliant

Prepare & Plan

- Are your systems FAR 52.204-21 and/or NIST 800-171 compliant? What is your current SPRS score?
- Do you need to build a new CUI enclave? Can you buy an inherited SaaS environment (PreVeil, Box.com etc.)?
- If you are on Microsoft Commercial – know that it is not compliant for CUI, and you will need to consider GCC/GCC High.
- If you are on Google, you will need to consider the Google Gov platform or an overlay SaaS solution.
- Are you storing CUI in your ERP/Business Systems? You need to know before planning your architecture

Things a Contractor Can Do to Prepare for CUI Clauses

Ask Questions

- When the RFP has a Q&A session – ask questions!
- Will DFARS 7012 or DFARS 7021 be put on this Contract?
- Will this contract be exempt from DFARS 7012/7021 due to [COTS items or Commercial Items]?
- Will CMMC certification be required as a condition of contract award?
- Until the new FAR clause comes out – ask for the **Security Classification Guide** (once the FAR comes out, the SF-XXX form will take its place)

Don't Fail to Plan for Contingencies & Incidents

- You may receive CUI at any time so have a backup plan (PreVeil (Email/File Sharing solution) is a great option for this).
- Receive all email for any Federal/DoD contracts through a secured address – do not assume the Government knows where to safely send you CUI – they will send to the address they have on file.
- Put a header on your lower security side emails to prevent accidental CUI spills to unsecured systems: **"This email is not approved for the receipt or processing of CUI. To send CUI to [company] please address it to [secure-email@company.us]"**

Life Sciences Trends & Topics
WEBCAST SERIES

Life Sciences Industry Requirements

LIFE SCIENCES

Industry Requirements

Regulatory

HIPAA

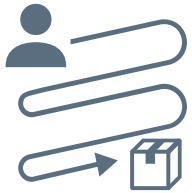
FDA

SOX

Business Continuity and Intellectual Property Protection

IP Protection

Proprietary Market

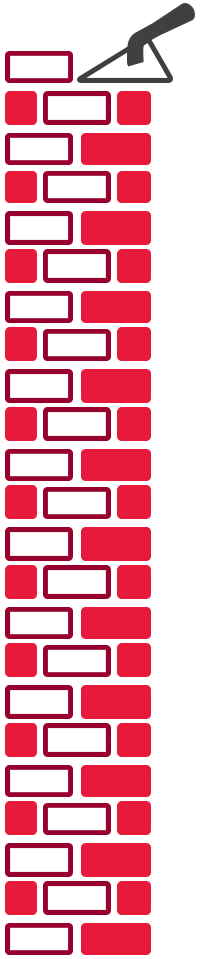


Supply Chain

Research Enclaves

INTERNET

BUSINESS SYSTEMS



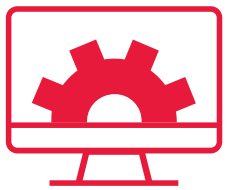
CLINICAL DATA

LAB SYSTEMS

MANUFACTURING SYSTEMS

Connected Systems

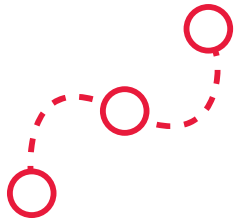
Today it is nearly impossible to disconnect all systems from the outside world. With cloud-based SaaS system being the norm, most systems cannot be simply disconnected.



ERP

QMS

MES



Serialization

LIMS

Connected Systems

Systems which are accessed over the web need additional security to ward off cyber security risks

Multi-factor Authentication (MFA)

Single Sign On (SSO)

SaaS Audits (SOC2)

Penetration Testing

Training

Vendor Contracts

Other Areas of Concern

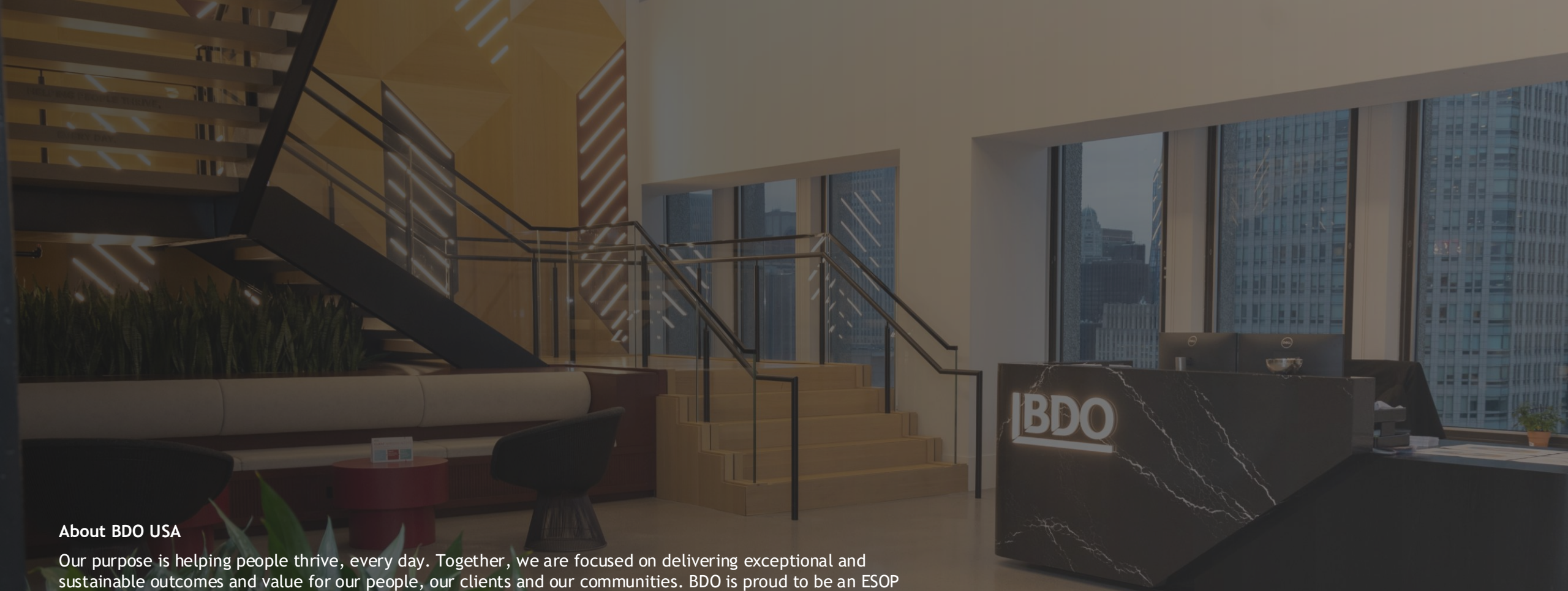
- Supply chain validation
- Vendor background checks
- Use of data centers
- Connected or Add-in Applications
- Hiring third-party consultants

M&A Activity

- Security due diligence in mergers and acquisitions
  - Look for consistency in security rules and application of those rules
  - Look for audit proof
- Emphasis on security during M&A processes

Life Sciences Trends & Topics
WEBCAST SERIES

Questions?



About BDO USA

Our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes and value for our people, our clients and our communities. BDO is proud to be an ESOP company, reflecting a culture that puts people first. BDO professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. For more information, please visit: www.bdo.com.