



The New Super-Soldier in the Global Trade War is in Your Healthcare Supply Chain

Julie Janeway, JD, MSA
Erica Powell Bell, JD
 SBM-HCLS Annual Meeting
 September 17, 2026

Copyright Julie Janeway 2026. All Rights Reserved

1

DISCLOSURE

The presenters have no significant financial interest/arrangements with any organization that could be perceived as a real or apparent conflict of interest with the subject matter of the presentation, participants, or the SBM - HCLS.

The opinions, materials, and statements presented are those of the presenters, except where otherwise noted.

2

2

ATTENTION PARTICIPANTS

WE ARE GOING TO MOVE VERY QUICKLY

- We are not going to read the slides or cover all points on the slides
- The PPT info is there as a reference and a useful Take-Home Resource
- **Sit back, listen, and try to absorb the information**
- **PLAN NOW** to educate your risk management and supply chain / procurement colleagues soon

3 DISCLAIMER: This is general information being provided to attendees for educational purposes, without knowledge of any attendee's organization's individual legal situation, and is not intended to, nor does it constitute specific legal advice to any attendee or attendee's organization.

3

2018: GAME ON
It started with tariffs.



TARIFFS
The first shots in a much bigger game.

TARIFFS + RETALIATION

U.S. Section 301 tariffs on Chinese goods; China imposes counter-tariffs.

Tariffs were only the opening move....

First: the product at the border.
Next: the company behind it.

4

2019-2020: TARGETING TECHNOLOGY
From products to companies and technology.



TELECOM + A TRADE DEAL

U.S. restricts exports to Huawei and other tech companies, cutting off its global component supply. They signed the Phase One Agreement that left many U.S. tariffs in place, and later strengthened many

It's no longer just what we import — but who we do business with.

5

2020-2022: SUPPLY CHAIN BATTLE
COVID showed who controls the supply chain.



SUPPLY CHAINS + CHIPS

U.S. supply-chain reviews and advanced-chip controls expand the focus.

Turns out, supply chains are a national security issue.

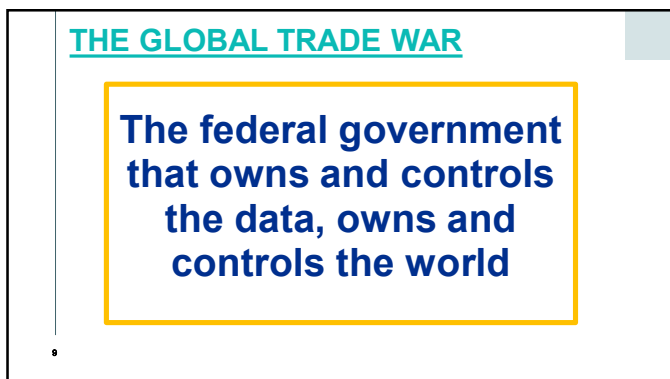
6



7



8



9

Definition: BIOTECHNOLOGY

Biotechnology includes healthcare and health-tech:

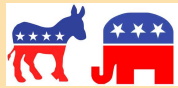
- Pharma / biopharma (biologics, biosimilars, monoclonal antibodies, therapeutic proteins)
- Vaccines
- Gene and cell therapies
- AI-driven drug discovery
- Diagnostics and “theranostics” (therapeutic diagnostics)
- The related research, and equipment, software, systems, or data needed to create, operate, or analyze any of the above

BIOTECH DATA ...

10

10

THE LEGISLATIVE LANDSCAPE



11

11

BIPARTISAN Support but *“Made in Michigan”*

It all starts here:

The National Defense Authorization Act (NDAA) for Fiscal Year 2026

– Passed into Law December 18, 2025 – Sen. Jack Reed, D-RI, Rep. Adam Smith, D-WA, Sen. Roger Wicker, R-MS, Sen. John Cornyn, R-TX, Rep. Mike Rogers, R-AL.

12

12

BIPARTISAN Support but "Made in Michigan"

- The National Defense Authorization Act (NDAA) for Fiscal Year 2026 - **The BIOSECURE Act** - Passed into Law December 18, 2025 – Sen. Gary Peters, D-MI, Rep. John Moolenaar, R-MI, Rep. Raja Krishnamoorthi, D-IL, Rep. Brad Wenstrup, R-OH, Sen. Bill Hagerty, R-TN, et al.
 - Rep. Mike Moolenaar is the Chairman of the House Select Committee on the Chinese Communist Party
- The primary purpose of the BIOSECURE Act is to protect U.S. national security, intellectual property, and American genomic data from exploitation by foreign adversaries (specifically targeting entities tied to China).
- It prohibits U.S. federal executive agencies from buying or obtaining biotechnology equipment, software, or services from designated "Biotechnology Companies of Concern" (BCCs). Applies to Prime Contractors, Federal grant holders, Federal Loan holders (not student loans), Cooperative Agreement holders, and all related FDRs, and their FDRs, worldwide.

13

13

BIPARTISAN Support but "Made in Michigan"

- The National Defense Authorization Act (NDAA) for Fiscal Year 2026 - **The Comprehensive Outbound Investment National Security Act of 2025 (COINS Act)** – Passed into Law December 2025 – Rep. John Moolenaar, R-MI, Rep. Andy Barr, R-KY, Sen. John Cornyn, R-TX.
- The statute provides a permanent statutory framework that builds on previous executive branch efforts to ensure American dollars and retirement funds do not inadvertently fund or advance the military, cyber, or surveillance capabilities of foreign adversaries. It regulates investments in sensitive tech like AI and semiconductors.

14

14

BIPARTISAN Support but "Made in Michigan"

- The BINSAs Amendments to the COINS Act (Proposed May 19, 2026) – Rep. John Moolenaar, R-MI, Rep. Debbie Dingell, D-MI, Sen. Elissa Slotkin, D-MI, Sen. Pete Ricketts, R-NE.
- BINSAs adds biotechnology—specifically pharmaceutical development, biologics manufacturing, and clinical research—to the Treasury Department's restricted screening list, capturing equity investments, licensing deals, and joint ventures in the net.

15

15

BIPARTISAN Support but *"Made in Michigan"*

- **The Securing Innovation and Research from Adversaries (SIRA) Act** (Proposed May 13, 2026) – Rep. John Moolenaar, R-MI, Sen. Jim Banks, R-IN.
- The purpose of the SIRA Act is to prohibit the use of federal research funds for collaborations with blacklisted foreign entities or individuals linked to military-civil fusion strategies in countries like China.

16

16

BIPARTISAN Support but *"Made in Michigan"*

- **The Connected Vehicle Security Act** (Proposed April 29, 2026) – Sen. Elissa Slotkin, D-MI, Rep. John Moolenaar, R-MI, Rep. Debbie Dingell, D-MI, Sen. Bernie Moreno, R-OH.
- The legislation restricts the importation, manufacture, and sale of "connected" vehicles, as well as related automotive software and hardware components, that are linked to foreign adversaries like China, Russia, Iran, or North Korea. Its goal is to safeguard American drivers' data, protect domestic transportation infrastructure from foreign exploitation, and defend the U.S. automotive industry.

17

17

BIPARTISAN Support but *"Made in Michigan"*

- **The Promoting United States Wireless Leadership Act** (Proposed July 14, 2025) – Rep. Debbie Dingell, D-MI, Rep. Tim Walberg, R-MI, Rep. Tom Kean Jr., R-NJ, Rep. Yvette Clark, D-NY.
- The primary purpose of the Promoting United States Wireless Leadership Act is to maintain and bolster American leadership in the development of next-generation wireless communication networks (such as 5G, 6G, and future Wi-Fi protocols).

18

18

Also Getting on the Bipartisan Bandwagon....

- **The Biological IP Protection (BIPPA) Act** (Proposed December 11, 2025) – Sen. Tom Cotton, R-AR, Sen. Maggie Hassan, D-NH, Sen. Ted Budd, R-NC, Rep. Warren Davidson, R-OH, Rep. Chrissy Houlahan, D-PA.
- BIPPA directs the Department of Commerce to restrict the export of sensitive digital data sequences, such as human or AI-designed synthetic DNA and RNA, to "foreign entities of concern" (primarily targeting the People's Republic of China) to prevent industrial espionage and protect U.S. biotechnology innovations.

19

19

Also Getting on the Bipartisan Bandwagon....

- **The Countering Chinese Cyberthreats for Patients (Countering CCP) Act** (Proposed June 24, 2026) – Sen. Tom Cotton, R-AR.
- The primary purpose of the Countering Chinese Cyberthreats for Patients Act (also known as the Countering CCP Act) is to protect American healthcare infrastructure, patient safety, and data privacy by mitigating cybersecurity risks from Chinese-manufactured medical hardware.

20

20

Also Getting on the Bipartisan Bandwagon....

- **The China Technology Transfer Control Act** (Proposed February 7, 2025) – Sen. Josh Hawley, R-MO, Rep., Mark Green, R-TN.
- The primary purpose of the China Technology Transfer Control Act is to protect U.S. national and economic security by stopping sensitive American technologies and intellectual property (IP) from being acquired, transferred to, or exploited by the People's Republic of China (PRC).

21

21

Also Getting on the Bipartisan Bandwagon....

- **The Preventing PLA Acquisition of U.S. Technology Act** (Proposed May 14, 2025) – Sen. Jim Banks, R-IN, Sen. Marco Rubio, R-FL, Rep. Jim Banks, R-IN (during his time in the House).
- The primary purpose of the Preventing PLA Acquisition of U.S. Technology Act is to protect American national security by blocking the Chinese military from acquiring or benefiting from advanced U.S. technology, research, and intellectual property.

22

22

Also Getting on the Bipartisan Bandwagon....

"The Chips Act Procurement Bans"

- **The Chip Equipment Quality Integrity Protection Act ["The CHIP EQUIP Act"]** (Proposed November 20, 2025) – Sen. Mark Kelly, D-AZ, Sen. Marsha Blackburn, R-TN, Rep. Zoe Lofgren, D-CA, Rep. Jay Obernolte, R-CA, Rep. Frank Lucas, R-OK.
- The primary purpose of the Chip EQUIP Act is to protect American semiconductor supply chains by ensuring federal funds do not subsidize the chip manufacturing capabilities of foreign adversaries.

23

23

Also Getting on the Bipartisan Bandwagon....

"The Chips Act Procurement Bans"

- **The Federal Acquisition Rule (FAR) 5949 that bans the U.S. government from procuring electronic products or services that incorporate semiconductors made by specific Chinese entities** (Passed as part of the NDAA for Fiscal Year 2023, Initially Effective February 17, 2026, with full Effect December 23, 2027) – authorized by the passage of the National Defense Authorization Act for Fiscal Year 2023, and led by Sen. Chuck Schumer, D-NY, and Sen. John Cornyn, R-TX.

24

24

Also Getting on the Bipartisan Bandwagon....

- **DOJ's final rule Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons** (Effective April 8, 2025)
- The regulation prohibits or heavily restricts American companies and individuals from executing commercial data transactions that would give "Countries of Concern"—specifically **China, Russia, Iran, North Korea, Cuba, and Venezuela**—or entities under their control access to bulk quantities of Americans' personal details (*like genomic, biometric, health, financial, and precise geolocation data*).

26

25

The United States



v



China

28

The following are the positions and opinions of the respective countries only.

26

The U.S. and China on the Biotech World Stage

- **The United States is currently the world's overall biotechnology leader because of its:**
 - unmatched innovation ecosystem
 - world-class research institutions
 - venture capital
 - global regulatory influence

27

27

The U.S. and China on the Biotech World Stage

- China has emerged as the United States' principal strategic competitor through unprecedented government investment, rapid advances in biotechnology research and manufacturing, and leadership in several specialized areas.
- China is currently estimated to be only 2.7% behind the U.S. in biotechnology advancement, production, and research. One of the most widely used open AI programs currently available on the planet – DeepSeek – is a recognized core element of China's national strategic infrastructure.

28

28

The U.S. and China on the Biotech World Stage

- The National Security Commission on Emerging Biotechnology (NSCEB) states that China has currently taken over leadership in:
 - global clinical trials, deal value, and clinical output (SynBioBeta)
 - speed to market on new innovations (various industry analyses)
 - R&D Spending (NIIST)
- It projects that Chinese-developed drugs will account for 35% of all U.S. FDA approvals by 2040.
- NSCEB declared in major strategic briefings that China is projected to challenge or take over the U.S. for leadership in all sectors of biotech by the end of 2028.

29

29

The U.S. on the Biotech World Stage



- The increasing tension between the countries is a declared national security issue.
- The U.S. government's position is that China engages in theft of U.S. and other countries' data and intellectual property, there is a military-civil fusion of the Chinese biotech industry with the Chinese Communist government, and it systemically exploits significant global supply chain vulnerabilities to collect data, violate IP rights, and steal other assets.
- The U.S. government has claimed as a particular concern that data collected by Chinese biotech firms could be used for advanced human bioweapons, agricultural and environmental bioweapons, ethnic-specific genetic targeting, or foreign surveillance, among others.

30

30

The U.S. on the Biotech World Stage



The U.S. has alleged that Chinese entities have obtained proprietary biotechnology information through:

- Cyber intrusions (hacking) into companies and research institutions
- Insider theft by employees or collaborators (e.g., Edward Snowden, and another from the same major U.S. Contractor just last year!)
- Unauthorized transfer of confidential research
- Misappropriation of IP / trade secrets
- Widespread data scraping of massive open data sources like clinical trial information and other major databases – often used to train AI
- Unauthorized copying of other proprietary databases

31

31

China on the Biotech World Stage



- China denies that these are legitimate or existing threats, and has characterized them as “outlandish falsehoods,” “baseless slanders,” “political manipulation,” “weaponization of trade practices,” and “brute-force protectionism disguised as national security.” It has called the U.S. “the world’s largest hacking and eavesdropping entity” citing an obvious double-standard in its argument.
- The Chinese government’s official position is that as the world’s two largest tech superpowers, they should abandon zero-sum thinking, avoid technical coercion, and work together to establish stable international rules and global technical and commercial practices for sharing data and information.

32

32

China on the Biotech World Stage



- It asserts that it is being targeted solely because its successful private enterprises are outcompeting American rivals.
- China has now instituted its own regulatory and counter-sanctions framework aimed primarily at the U.S., but also often at the European Union, Japan, and South Korea as well – all major biotech powerhouse countries ... and U.S. allies.

33

33

The U.S. and China on the Biotech World Stage

- Biotechnology is often treated differently from many other industries because it involves **dual-use technology that may have both civilian and national security/defense applications**, such as:
 - Human genomic **data**
 - Public health infrastructure **data**
 - Critical medicine, treatments, and related equipment **data**
 - Pandemic preparedness **data**
 - Food security **data**
 - Consumer use **data**
 - Agricultural biotechnology **data**
 - Bio-industrial manufacturing **data**
 - Geo-location tracking **data**

NATIONAL CRITICAL INFRASTRUCTURE

34

34

The U.S. and China on the Biotech World Stage

Examples of targeted information include:

- Drug development research
- Biologic manufacturing methods
- Cell and gene therapy technologies
- Vaccine technologies
- Proprietary algorithms
- Clinical trial information
- Manufacturing processes
- Intellectual property

35

35

The U.S. and China on the Biotech World Stage

U.S. Enforcement Efforts:

- Tariffs
- Import/export bans
- Placement of nationally owned or controlled entities on various banned lists like OFAC (that freezes all assets the entity holds under U.S. jurisdiction)
- Capital market and tech stack access restrictions and software controls
- Visa and travel bans
- The U.S. Department of Justice has brought criminal cases involving alleged theft of biotechnology trade secrets from U.S. companies and universities.

These cases involve individuals and should not be interpreted as evidence that all Chinese researchers or institutions engage in such conduct.

36

36



37

The “Lists”

The Existing Banned or Restricted Entities and Companies of Concern Lists

Department of the Treasury (OFAC)

The Office of Foreign Assets Control (OFAC) manages one of the heaviest, most restrictive blacklists. Violating these restrictions can carry severe civil and criminal penalties.

- **Specially Designated Nationals and Blocked Persons List (SDN):** Blocks assets and generally prohibits all transactions for targeted individuals, groups, and entities like terrorists, narcotics traffickers, and country-specific sanction targets.

38

The “Lists”

Department of Commerce - Bureau of Industry and Security (BIS)

- **BIS Entity List:** restricts the export, re-export, or transfer of sensitive items to foreign entities that pose a risk to U.S. national security or foreign policy.
- **Denied Persons List:** Bans specific individuals and companies from participating in export transactions regulated by the Export Administration Regulations (EAR).
- **Unverified List (UVL):** Lists foreign parties where BIS could not verify end-users or check legitimacy, triggering "red flags" for exporters.

39

The "Lists"

Department of State

- **ITAR Debarred Parties (AECA Debarred List):** Prohibits companies and individuals from participating in the export of defense articles and defense services under the International Traffic in Arms Regulations (ITAR).
- **Nonproliferation Sanctions List:** Targets foreign persons and entities sanctioned for engaging in the proliferation of weapons of mass destruction.

40

40

The "Lists"

Department of State

- **ITAR Debarred Parties (AECA Debarred List):** Prohibits companies and individuals from participating in the export of defense articles and defense services under the International Traffic in Arms Regulations (ITAR).
- **Nonproliferation Sanctions List:** Targets foreign persons and entities sanctioned for engaging in the proliferation of weapons of mass destruction.

41

41

The "Lists"

Department of Defense (DoD)

- **DoD 1260H and 1286 Lists:** Identifies "Chinese military companies" and other entities operating in or with the U.S. that are tied to the Chinese military or national security concerns.

42

42

The “Lists”

The Federal Communications Commission (FCC)

- **FCC Covered List:** Identifies telecommunications, video surveillance, and networking equipment or services that pose an unacceptable risk to U.S. national security.

43

43

The “Lists”

The Federal Communications Commission (FCC)

- **FCC Covered List:** Identifies telecommunications, video surveillance, and networking equipment or services that pose an unacceptable risk to U.S. national security.

44

44

The “Lists”

General Services Administration & Federal Procurement

- **System for Award Management Exclusions (SAM):** (The former EPLS List). Identifies contractors debarred, suspended, or otherwise excluded from receiving federal government contracts or subcontracts.

45

45

The "Lists"

NEW: Office of Management and Budget (OMB)

- **Biotechnology Companies of Concern (BCC List):** To be established by December 2026, which will trigger the start of regulatory drafting including FARs and DFARs. It will be based primarily, although not exclusively, off the DoD 1260H and 1286 Lists, BIS Entity List, and OFAC, GSA, and FCC lists. Foreign adversary companies or individuals' ownership and/or control limits are expected to be zero percent to avoid inclusion on the BCC. This absolute threshold is likely where the challenge and opposition regarding inclusion on the list will occur....

46

46

Now...Back to The BIOSECURE Act....

47

The following are the positions and opinions of the respective countries only, not those of the presenters.

47

The BIOSECURE Act

- Designed as a major supply chain security measure.
- It restricts U.S. federal agencies, government contractors (and their downstream and related entities [their support goods and services supply chains], and grant, loan, and cooperative agreement recipients from utilizing biotechnology equipment and services (the "catch-all" provision) provided by foreign adversarial entities (China and North Korea, Russia, Cuba, Venezuela, and Iran), or entities with prohibited levels of ownership or control by entities or persons from these countries.
- The Act establishes a rigorous compliance framework aimed at separating U.S. federal biotech, healthcare, research and other funding source dollars from "Biotechnology Companies of Concern" (BCCs).

48

48

The BIOSECURE Act

WHO?

- **Direct Government Procurement:** U.S. federal agencies are explicitly barred from buying or obtaining biotechnology equipment, information, data, products, or services from any designated BCC.
- **Contractor Restrictions:** The government cannot enter into, renew, or extend contracts with any company that uses BCC equipment, software, data, or services to perform that contract. This forces pharmaceutical, life sciences, and healthcare entities to thoroughly audit their supply chains.
- **Funding Prohibitions:** Federal contracts, loans, grants, and cooperative agreements cannot be utilized to fund or procure products or services from a BCC list entity, [which heavily impacts universities and research institutions](#).

49

49

The BIOSECURE Act

WHAT?

- The statutory definitions are incredibly broad, given the stated intent of the Act.
- "Biotechnology equipment or services" includes, but is certainly not limited to:
 - genomic sequencing platforms
 - analytical software/firmware
 - data storage
 - bioinformatics and statistical analysis tools
 - data brokerage
 - research and information procurement or supply
 - multiomic processing
 - research
 - analysis equipment
 - support, consulting, or contract development and manufacturing organization (CDMO) services

50

50

The BIOSECURE Act

WHY?

Because if you are part of the supply chain eco-system of a federal contract, research grant, federal loan, or federal cooperative agreement, you are going to be required to:

- Certify, with records of traceability, to the federal government that your supply chain does not have connections to any entity or person on the BCC List (or any other list).
- And if you are the prime contractor, or grant, loan, or cooperative agreement recipient, you [are responsible for your entire supply chain also certifying](#) to the government with traceability records.... OR get them out of your supply chain.

51

51

The BIOSECURE Act

WHEN?

- The BCC list is required to be developed by December 2026.
- Within 180 days of the BCC publication, OMB must issue formal binding implementation guidance for federal agencies.
- Within 1 year of guidance issuance the Federal Acquisition Regulatory Council must finalize revisions to the relevant FARs to integrate statutory prohibitions.
- To prevent severe disruptions to the pharmaceutical supply chain and drug availability, the law includes a 5-year grandfathering period for major existing contracts.
- Companies entering new contracts, or whose contracts will renew or option years will kick in, generally have until 2028 or until renewal date or options arise to fully decouple and transition to alternative providers, though preparations should begin immediately.
- The federal government is prohibited from engaging any contract, grant, loan, or cooperative agreement without BIOSECURE compliance after the implementation date, without a legitimate exception provided by the Act.

52

52

The BIOSECURE Act

APPLICABLE STANDARDS:

- While there are no specific ISO, accreditation, or other standards required by the text of the Act, companies navigating BIOSECURE compliance will likely rely on several key standards to meet the Act's strict supply chain, risk management, and data protection requirements, among others:
 - ISO/IEC 17025 – The standard for Testing and Calibration Laboratories
 - ISO 9001 – The standard for Quality Management Systems
 - ISO/IEC 27001 – The standard for Information Security Management
 - ISO/IEC 27701 – the standard for Privacy Information Management
 - ISO 28000:2022 – The standard for Supply Chain Security Management
 - ISO 13485 – The standard for Quality Management Systems in Medical Devices
 - ISO 44001 – The standard for Collaborative Business Relationship Management

53

53

IDENTIFYING YOUR “SUPER SOLDIERS”



54

54

The “Super Soldiers”

The “Super Soldiers” in this global trade war are:

- Data, information, and research
- AI
- Biotech
 - Medical and Healthcare
 - Agriculture and Food Production
 - Industrial and Manufacturing
 - Marine and Aquatic
 - Environmental and Nutritional

55

55

The “Super Soldiers”

Have you identified the domestic or internationally acquired, supported, or produced “Super Soldiers” in your operations and supply chain?

- Those products, services, personnel, companies, or components that your organization relies on – going in or out of the organization
- Are they critical to operations?
- Can they be sourced elsewhere?
- Do they have any relation, at any level, to any federal contract, research grant, federal loan, or federal cooperative agreement?

56

56

The “Super Soldiers”

Do the “Super-Soldiers” in your supply chain belong to the U.S. or to a foreign adversary country?

Is your organization heavily reliant on or significantly involved with:

- deep and broad supply chains
- internationally manufactured, procured, developed, brokered, supplied products/components, services, data, research, intellectual property, etc.
- research involving international cooperation
- research using or sharing produced or procured data sets
- independent contractor companies and/or personnel

57

57

The “Super Soldiers”

Does your organization, and/or do your supply chain organizations, only consider cost when purchasing goods and services?

Could you track your relevant supply chains right now if you had to?

Could you track pharmaceuticals beyond the wholesale distributor you buy them from?

Does your organization, (or your clients' organizations) ever check suppliers and vendors against any of the existing banned lists?

58

58

The “Super Soldiers”

Bonus Questions:

1. What level of background checking and exclusion list checking is performed for your entire supply chain?
2. What level of security is applied to business with your entire supply chain, including employees and contractors of those supply chain entities?
3. What level of scrutiny and security is applied to supply chain relationships specifically involving any use or sharing of clinical, scientific, research, healthcare, or other data?
4. What level of scrutiny is applied to the hiring of any persons who will work on research or clinical trial projects (let alone on anything else involving purchasing or data)?

59

59

The “Super Soldiers”

And the final two mind-blowing questions of the day.....

- Does anyone at your organization have any idea what any and every organization in your supply chain is doing about any of these same questions regarding their own supply chains?
- Have you budgeted for personnel and resources to start tracking down all this information over the next 18-24 months?

60

60

The “Super Soldiers”

Start Now:

- You have been given the basics
- We have provided a simple readiness assessment check list to get you organized and moving forward
- We have provided a simple overview of all the branches of biotech “Super Soldiers,” because they all affect each other ... and all of us on the planet
- **Contact us if you need help!**

61

61

In Conclusion

The trade war is raging, and it is only getting worse by the moment because:

The federal government that owns and controls the data, owns and controls the world

62

62

In Conclusion

And the Super Soldiers of this trade war are engaged in a battle to the death in your own backyard



63

63



64

**Thank
you**



If you need assistance with BIOSECURE
or other biotech-related legislation
compliance on behalf of your
organization or that of a client, contact:

Julie Janeway, JD, MSA

517-667-1783

jhilljaneway@wm.edu

jjaneway@advizehealth.com

65
