



BOIES SCHILLER FLEXNER

A black and white photograph of a city skyline, likely Los Angeles, featuring several tall skyscrapers and palm trees in the foreground. The image is partially obscured by a dark blue diagonal shape on the right side of the slide.

## Hot Topics in Compliance

**David K. Willingham**  
**Jalle Dafa**


**October 29, 2019**

An illustration in a muted blue and grey color palette. In the background, several stylized, rounded figures are depicted. On the left, two figures carry large money bags with dollar signs (\$) on them. On the right, two figures carry rectangular signs; one says 'TECHNOLOGY' and the other says 'LICENSING FEE'. A third figure on the far right is partially visible, also carrying a sign. The entire scene is set against a light blue background with a dark blue, textured ground area at the bottom.

## IP USE, TRANSPORT, & THEFT

## IP USE, TRANSPORT, AND THEFT

- Trump Administration's Approach
- Three recent letters from Department of Defense and White House Office of Science and Technology Policy:



**THE UNDER SECRETARY OF DEFENSE**  
3030 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3030

**MAR 20 2019**

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT  
ASSISTANT SECRETARY OF DEFENSE FOR ACQUISITION  
SERVICE ACQUISITION EXECUTIVES  
SPECIAL OPERATIONS COMMAND


SUBJECT: Actions for the Protection of Intellectual Property, Controlled Information, Key Personnel and Critical Technologies

The National Defense Authorization Act (NDAA) for FY 2019, Section 1286, pages 443-445, directs the Secretary of Defense to establish an initiative to work with academic institutions who perform defense research and engineering activities:

1. To support protection of intellectual property, controlled information, key personnel, and information about critical technologies relevant to national security; and
2. To limit undue influence, including through foreign talent programs, by countries to exploit United States technology within the Department of Defense research, science and technology, and innovation enterprise.

I direct that Department of Defense (DoD) Grants Managers and other personnel supporting the award and administration of grants, cooperative agreements, Technology Investment Agreements, and other non-procurement transactions shall take the following actions for all research and research-related educational activities supported by these types of DoD instruments.

1. Thirty business days after the date of this issuance, all new DoD Notices of Funding Opportunities (NFOs) pertaining to research and research-related educational activities shall include the following requirements:
  - a. Proposers shall submit the below information for all key personnel, whether or not the individuals' efforts under the project are to be funded by the DoD:
    - A list of all current projects the individual is working on, in addition to any future support the individual has applied to receive, regardless of the source.
    - Title and objectives of the other research projects.
    - The percentage per year to be devoted to the other projects.
    - The total amount of support the individual is receiving in connection to each of the other research projects or will receive if other proposals are awarded.
    - Name and address of the agencies and/or other parties supporting the other research projects.
    - Period of performance for the other research projects.



EXECUTIVE OFFICE OF THE PRESIDENT  
OFFICE OF SCIENCE AND TECHNOLOGY POLICY  
WASHINGTON, D.C. 20502

September 16, 2019

**Letter to the United States Research Community**


Dear Colleagues,

As a fellow researcher and former university vice president for research, I know firsthand that the open and internationally collaborative nature of the United States research enterprise has been critical to our success in research, and that this success has underpinned our Nation's prosperity and security. Indeed, the values we cherish as Americans are the ethos of research itself: namely, the freedom to explore new frontiers, the commitment to openness and transparency through the sharing of methods and results, the ability to debate difficult issues thoughtfully and with civility, and the passion to work with and improve the lives of others. By adhering to these values and operating with due regard to principles of integrity – including reciprocity, openness, and transparency – your work has made America the world leader in science and technology. The Nation is indebted to you.

Yet we must not take our research enterprise or its global leadership position for granted. Over the past several years, some nations have exhibited increasingly sophisticated efforts to exploit, influence, and undermine our research activities and environments. As researchers, we must acknowledge the changing geopolitical and international scientific landscape: United States policies and practices must evolve thoughtfully and appropriately to meet current and future challenges. The success of our research enterprise is dependent on everyone upholding the principles of research.

Some of those recent efforts to exploit America's research enterprise have come through foreign government-sponsored talent recruitment programs. Historically, researchers at United States institutions could in many cases participate in a talent program and simultaneously receive both foreign and United States government support. Under some circumstances, this may still be acceptable. However, it has become clear that features of some talent programs are unacceptable and inconsistent with our research values and research principles. Breaches of research ethics, both within talent programs and more generally, include the failure to disclose required information such as foreign funding, unapproved parallel foreign laboratories (so-called shadow labs), affiliations and appointments, and conflicting financial interests. Other inappropriate behaviors include conducting undisclosed research for foreign governments or companies on United States agency time or with United States agency funding, diversion of intellectual property or other legal rights, and breaches of contract and confidentiality in or surreptitious gaming of the peer-review process.

Ultimately, these inappropriate behaviors, whether or not they arise through participation in a foreign talent program, interfere with the allocation of Federal funding in a fair manner based on merit. As a result, these breaches of research security and integrity position others to reap the benefits of your hard work without bearing the associated risks or making the investments borne by American taxpayers and other funders. These activities ultimately undermine the integrity of the research enterprise and, thus, our economic and national security.



**THE UNDER SECRETARY OF DEFENSE**  
3030 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3030

**OCT 10 2019**

Dear Academic Colleagues:

For decades, scientists at universities and research centers, supported by the Department of Defense (DoD), have made ground-breaking scientific discoveries that underpinned dramatic commercial and national security advances, significantly improving the lives of citizens here and abroad. DoD recognizes the contribution of research integrity principles, such as the free exchange of ideas, transparency, and collaboration across research communities as critical to our mutual success. Yet today, the ability to make similar advances is at risk, and research integrity is jeopardized through foreign governments' exploitation that intentionally target U.S. and allied partner research and intellectual capital.

We must find ways to protect research integrity that has contributed to the creation of the finest research institutions in the world and allows us to attract the necessary talent to maintain our economic and national security. The principles of integrity, openness, reciprocity, merit-based competition, and transparency are the foundation of American innovation. The theft of controlled information and unethical diversion of intellectual capital threatens both the American economy and the security of our nation. I request your assistance to preserve the long-standing norms and ethical behaviors that have benefited our research institutions.

The challenge of protecting the integrity of our research enterprise is a national priority. In his September 16, 2019, letter<sup>1</sup> to the research community, Dr. Kelvin Droegemeier, Director of the White House Office of Science and Technology Policy (OSTP), described a new OSTP-led interagency Joint Committee on the Research Environment (JCORE). DoD is an active participant in JCORE, and in its sub-committee on Research Security, which is initially focused on coordinating four lines of Federal effort: coordinating outreach and engagement; disclosure requirements for participation in federally funded research; best practices for academic research institutions; and methods for identification, assessment, and management of risk. This work will help agencies that fund Federal research to develop common standards for identifying and adjudicating conflicts of interest and conflicts of commitment from these disclosures. It will also help agencies that fund Federal research to clarify consequences for failing to make these disclosures.

Even prior to the establishment of JCORE, DoD has taken several steps to address this rising threat and protect open research at U.S. institutions. In October 2018, the Secretary of Defense formed the Protecting Critical Technology Task Force to work across the defense industry and research enterprise toward these goals. On March 20, 2019, to address conflicts of interest and conflicts of commitment, I signed a memorandum<sup>2</sup> requiring that all research and research-related educational activities conducted through DoD research grants, cooperative agreements, Technology Investment Agreements, and other non-procurement transactions require key personnel to disclose

<sup>1</sup> <https://www.whitehouse.gov/wp-content/uploads/2019/09/OSTP-letter-to-the-US-research-community-september-2019.pdf>

<sup>2</sup> Dr. Michael D. Griffin, Under Secretary of Defense for Research and Engineering, Memorandum titled "Actions for the Protection of Intellectual Property, Controlled Information, Key Personnel and Critical Technologies," dated March 20, 2019.





THE UNDER SECRETARY OF DEFENSE  
3030 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3030

MAR 20 2019

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT  
ASSISTANT SECRETARY OF DEFENSE FOR ACQUISITION  
SERVICE ACQUISITION EXECUTIVES  
SPECIAL OPERATIONS COMMAND

SUBJECT: Actions for the Protection of Intellectual Property, Controlled Information, Key Personnel and Critical Technologies

The National Defense Authorization Act (NDAA) for FY 2019, Section 1286, pages 443-445, directs the Secretary of Defense to establish an initiative to work with academic institutions who perform defense research and engineering activities:

1. To support protection of intellectual property, controlled information, key personnel, and information about critical technologies relevant to national security; and
2. To limit undue influence, including through foreign talent programs, by countries to exploit United States technology within the Department of Defense research, science and technology, and innovation enterprise.

I direct that Department of Defense (DoD) Grants Managers and other personnel supporting the award and administration of grants, cooperative agreements, Technology Investment Agreements, and other non-procurement transactions shall take the following actions for all research and research-related educational activities supported by these types of DoD instruments:

1. Thirty business days after the date of this issuance, all new DoD Notices of Funding Opportunities (NFOs) pertaining to research and research-related educational activities shall include the following requirements:
  - a. Proposers shall submit the below information for all key personnel, whether or not the individuals' efforts under the project are to be funded by the DoD:
    - A list of all current projects the individual is working on, in addition to any future support the individual has applied to receive, regardless of the source.
    - Title and objectives of the other research projects.
    - The percentage per year to be devoted to the other projects.
    - The total amount of support the individual is receiving in connection to each of the other research projects or will receive if other proposals are awarded.
    - Name and address of the agencies and/or other parties supporting the other research projects.
    - Period of performance for the other research projects.



EXECUTIVE OFFICE OF THE PRESIDENT  
OFFICE OF SCIENCE AND TECHNOLOGY POLICY  
WASHINGTON, D.C. 20502



RESEARCH  
AND ENGINEERING

THE UNDER SECRETARY OF DEFENSE  
3030 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3030

MAR 20 2019

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT  
ASSISTANT SECRETARY OF DEFENSE FOR ACQUISITION  
SERVICE ACQUISITION EXECUTIVES  
SPECIAL OPERATIONS COMMAND

SUBJECT: Actions for the Protection of Intellectual Property, Controlled Information, Key Personnel and Critical Technologies

The National Defense Authorization Act (NDAA) for FY 2019, Section 1286, pages 443-445, directs the Secretary of Defense to establish an initiative to work with academic institutions who perform defense research and engineering activities:

1. To support protection of intellectual property, controlled information, key personnel, and information about critical technologies relevant to national security; and
2. To limit undue influence, including through foreign talent programs, by countries to exploit United States technology within the Department of Defense research, science and technology, and innovation enterprise.

March 20, 2019.



THE UNDER SECRETARY OF DEFENSE  
3030 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3030

OCT 10 2019

research centers, supported by the Department of Defense, have made significant discoveries that underpinned dramatic improvements in the lives of citizens here and abroad. These discoveries, such as the free exchange of research integrity principles, such as the free exchange of research communities as critical to our mutual advancement is at risk, and research integrity is a foundation that intentionally target U.S. and allied

integrity that has contributed to the creation of the new world. To attract the necessary talent to maintain our nation's leadership in science, technology, and innovation, we must ensure that the integrity of our research enterprise is a national priority. In the community, Dr. Kelvin Droegemeier, Director of the Office of Science and Technology Policy (OSTP), described a new OSTP-led environment (JCORE). DoD is an active participant in this environment, which is initially focused on coordinating research and engagement; disclosure requirements for research practices for academic research institutions; and management of risk. This work will help agencies that are working to identify and adjudicate conflicts of interest and disclosures. It will also help agencies that fund research to make these disclosures.

DoD has taken several steps to address this rising concern. In October 2018, the Secretary of Defense announced the creation of the Defense Research and Engineering (DRE) Force to work across the defense industry and research community to address conflicts of interest and ensure that all research and research-related research grants, cooperative agreements, Technology Investment Agreements, and other non-procurement transactions require key personnel to disclose

OSTP letter to the US research community - september 2018. Research and Engineering. Memorandum titled "Actions for the Protection of Intellectual Property, Controlled Information, Key Personnel and Critical Technologies," dated

MAR 20 2019

- A list of all current projects the individual is working on, in addition to future support the individual has applied to receive, regardless of the
- Title and objectives of the other research projects.
- The percentage per year to be devoted to the other projects.
- The total amount of support the individual is receiving in connection with the other research projects or will receive if other proposals are awarded.
- Name and address of the agencies and/or other parties supporting the research projects.
- Period of performance for the other research projects.



September 16, 2019

Dear Colleagues,

As a fellow researcher and former university vice president for research, I know firsthand that the open and internationally collaborative nature of the United States research enterprise has been



September 16, 2019

As a fellow researcher and former university vice president for research, I know firsthand that the open and internationally collaborative nature of the United States research enterprise has been critical to our success in research, and that this success has underpinned our Nation's prosperity and security. Indeed, the values we cherish as Americans are the ethos of research itself; namely, the freedom to explore new frontiers, the commitment to openness and transparency through the sharing of methods and results, the ability to debate difficult issues thoughtfully and with civility, and the passion to work with and improve the lives of others. By adhering to these values and operating with due regard to principles of integrity – including reciprocity, openness, and transparency – your work has made America the world leader in science and technology. The Nation is indebted to you.



OCT 10 2019

Dear Academic Colleagues:

ment of JCORE, DoD has taken several steps to address this rising U.S. institutions. In October 2018, the Secretary of Defense Technology Task Force to work across the defense industry and goals. On March 20, 2019, to address conflicts of interest and a memorandum\* requiring that all research and research-related through DoD research grants, cooperative agreements, Technology non-procurement transactions require key personnel to disclose

ry of Defense for Research and Engineering, Memorandum titled "Actions for Controlled Information, Key Personnel and Critical Technologies," dated



THE UNDER SECRETARY OF DEFENSE  
3030 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3030

MAR 20 2019

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT  
ASSISTANT SECRETARY OF DEFENSE  
SERVICE ACQUISITION EXECUTIVES  
SPECIAL OPERATIONS COMMAND

SUBJECT: Actions for the Protection of Intellectual Property, Critical Personnel and Critical Technologies

The National Defense Authorization Act (NDAA) for FY 2014, directs the Secretary of Defense to establish an initiative to work who perform defense research and engineering activities:

1. To support protection of intellectual property, controlled information and information about critical technologies relevant to national defense.
2. To limit undue influence, including through foreign talent exploit United States technology within the Department of Defense and technology, and innovation enterprise.

I direct that Department of Defense (DoD) Grants Managers supporting the award and administration of grants, cooperative agreements, and other non-procurement transactions shall for all research and research-related educational activities supported by instruments.

1. Thirty business days after the date of this issuance, all new Opportunities (NFOs) pertaining to research and research activities shall include the following requirements:
  - a. Proposers shall submit the below information for all key personnel whose efforts under the project are to be performed:
    - A list of all current projects the individual is working on that support the individual's efforts to receive, develop, or perform research projects.
    - Title and objectives of the other research projects.
    - The percentage per year to be devoted to the other research projects.
    - The total amount of support the individual is receiving in connection to each of the other research projects or will receive if other proposals are awarded.
    - Name and address of the agencies and/or other parties supporting the other research projects.
    - Period of performance for the other research projects.



RESEARCH  
AND ENGINEERING

Dear Academic Colleagues:

For decades, scientists at universities and research centers, supported by the Department of Defense (DoD), have made ground-breaking scientific discoveries that underpinned dramatic commercial and national security advances, significantly improving the lives of citizens here and abroad. DoD recognizes the contribution of research integrity principles, such as the free exchange of ideas, transparency, and collaboration across research communities as critical to our mutual success. Yet today, the ability to make similar advances is at risk, and research integrity is jeopardized through foreign governments' exploitation that intentionally target U.S. and allied partner research and intellectual capital.

As a result, these researchers are in a research security and integrity position where they are unable to enjoy the benefits of their hard work without bearing the associated risks or making the investments borne by American taxpayers and other funders. These activities ultimately undermine the integrity of the research enterprise and, thus, our economic and national security.



EXECUTIVE OFFICE OF THE PRESIDENT  
OFFICE OF SCIENCE AND TECHNOLOGY POLICY  
WASHINGTON, D.C. 20502

September 16, 2019

Letter to the United States Research Community

THE UNDER SECRETARY OF DEFENSE  
3030 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3030

OCT 10 2019



THE UNDER SECRETARY OF DEFENSE  
3030 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3030

OCT 10 2019

Dear Academic Colleagues:

For decades, scientists at universities and research centers, supported by the Department of Defense (DoD), have made ground-breaking scientific discoveries that underpinned dramatic commercial and national security advances, significantly improving the lives of citizens here and abroad. DoD recognizes the contribution of research integrity principles, such as the free exchange of ideas, transparency, and collaboration across research communities as critical to our mutual success. Yet today, the ability to make similar advances is at risk, and research integrity is jeopardized through foreign governments' exploitation that intentionally target U.S. and allied partner research and intellectual capital.

We must find ways to protect research integrity that has contributed to the creation of the finest research institutions in the world and allows us to attract the necessary talent to maintain our economic and national security. The principles of integrity, openness, reciprocity, merit-based competition, and transparency are the foundation of American innovation. The theft of controlled information and unethical diversion of intellectual capital threatens both the American economy and the security of our nation. I request your assistance to preserve the long-standing norms and ethical behaviors that have benefited our research institutions.

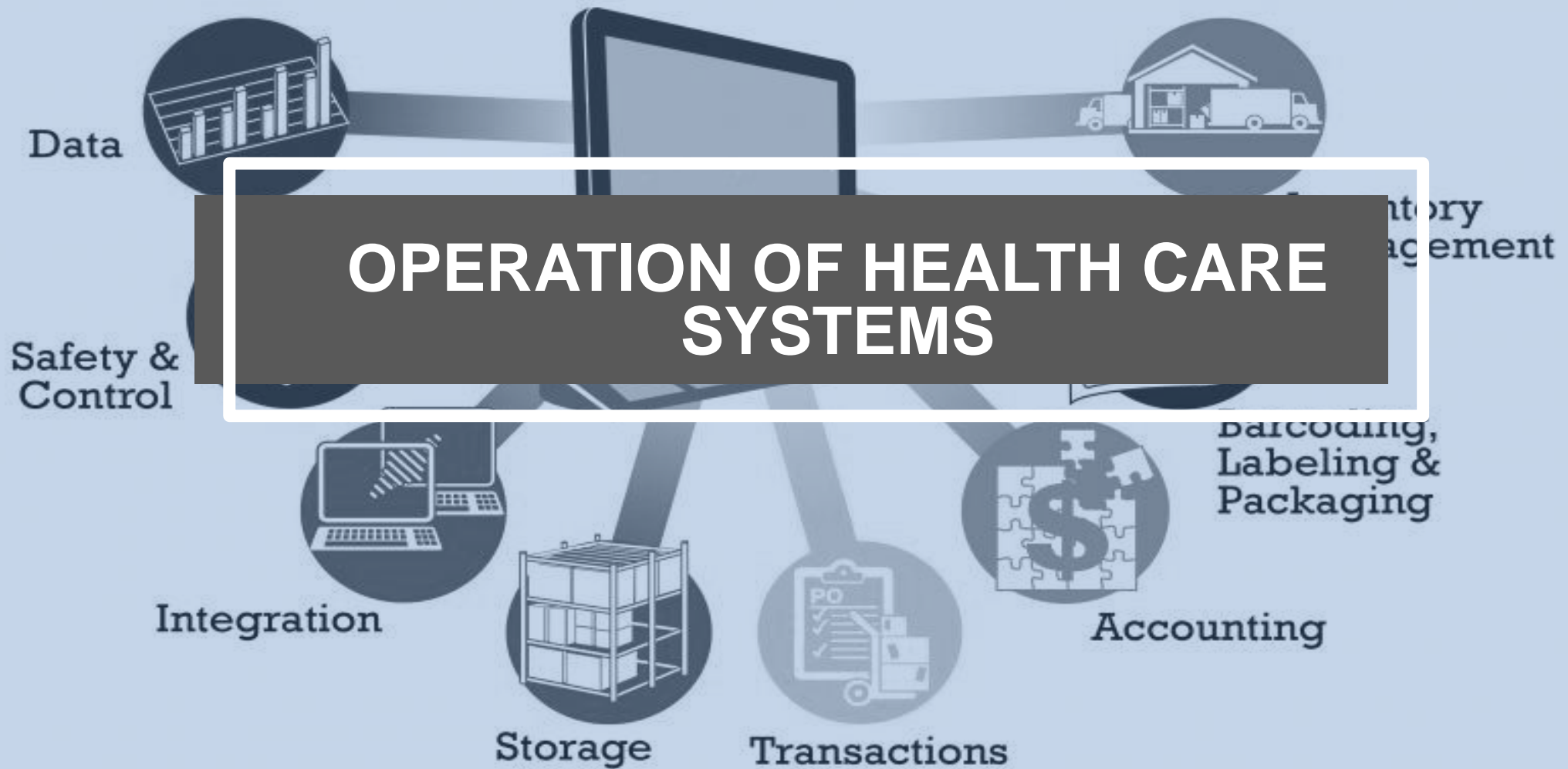
The challenge of protecting the integrity of our research enterprise is a national priority. In his September 16, 2019, letter<sup>1</sup> to the research community, Dr. Kelvin Droegemeier, Director of the White House Office of Science and Technology Policy (OSTP), described a new OSTP-led Interagency Joint Committee on the Research Environment (JCORE). DoD is an active participant in JCORE, and in its sub-committee on Research Security, which is initially focused on coordinating best practices for research security, including outreach and engagement, disclosure requirements for participation in federally funded research; best practices for academic research institutions; and methods for identifying, assessing, and managing risk. This work will help agencies that fund Federal research to develop common standards for identifying and adjudicating conflicts of interest and conflicts of commitment from these disclosures. It will also help agencies that fund Federal research to clarify consequences for failing to make these disclosures.

Even prior to the establishment of JCORE, DoD has taken several steps to address this rising threat and protect open research at U.S. institutions. In October 2018, the Secretary of Defense formed the Protecting Critical Technology Task Force to work across the defense industry and research enterprise toward these goals. On March 20, 2019, to address conflicts of interest and conflicts of commitment, I signed a memorandum<sup>2</sup> requiring that all research and research-related educational activities conducted through DoD research grants, cooperative agreements, Technology Investment Agreements, and other non-procurement transactions require key personnel to disclose

<sup>1</sup> <https://www.whitehouse.gov/wp-content/uploads/2019/09/OSTP-letter-to-the-US-research-community-september-2019.pdf>

<sup>2</sup> Dr. Michael D. Griffin, Under Secretary of Defense for Research and Engineering, Memorandum titled "Actions for the Protection of Intellectual Property, Controlled Information, Key Personnel and Critical Technologies," dated March 20, 2019.





## OPERATION OF HEALTH CARE SYSTEMS

---

- Data Protection and HIPAA
- Drug Diversion
- Telehealth

U.S. Attorneys » Central District of California » News

Department of Justice

U.S. Attorney's Office

Central District of California

---

FOR IMMEDIATE RELEASE

Thursday, February 21, 2019

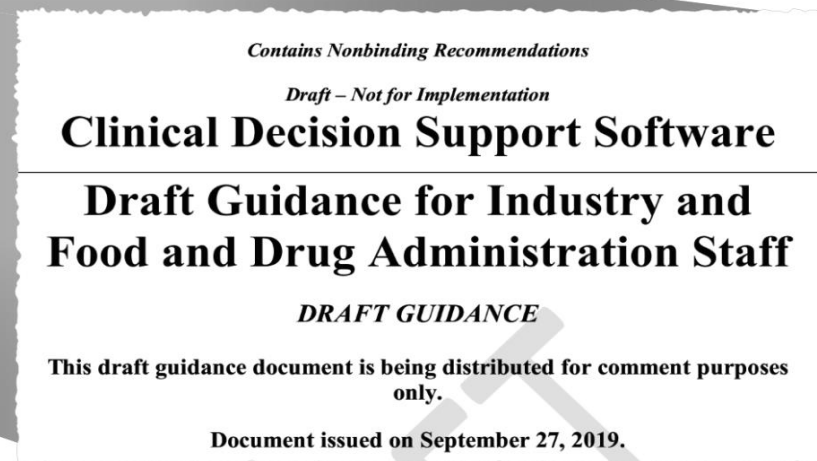
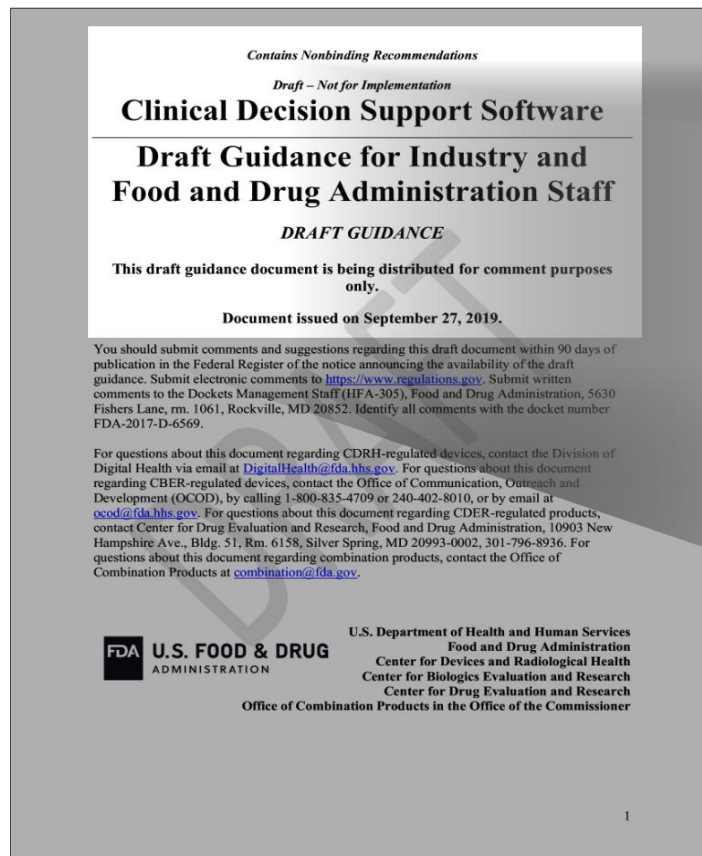
**DEA-Led Crackdown on Prescription Opioid Diversion Targets  
Medical Professionals with Criminal Charges, License  
Revocations**



## FDA REGULATIONS FOR AI

## FDA REGULATIONS FOR AI

- NEW Draft Guidance – Issued Sept 2019



## HIGHER EDUCATION ACT OF 1965



## HIGHER EDUCATION ACT OF 1965

---

- NEW proposed revisions to reporting requirements issued by DoE on September 6, 2019
- If requirements become final will significantly EXPAND the kind of gifts and contracts that must be reported

COMPLIANCE ALERT

OCTOBER 8, 2019

PROPOSED CHANGES TO HIGHER EDUCATION ACT OF 1965 §117 FOREIGN  
CONTRACTS AND GIFTS REPORTING REQUIREMENTS



## EXPORT CONTROLS

## EXPORT CONTROLS

- Trump administration IS enforcing controls
- Recent Example: charged UCLA professor faces **219 years**

Case 2:18-cr-00050-JAK Document 1 Filed 01/16/18 Page 1 of 82 Page ID #1

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the  
Central District of California

United States of America  
v.  
Yi-Chi Shih ("SHIH") and  
Kiet Ahn Mai ("MAI"),  
Defendant(s)

Case 2:18-cr-00050-JAK Document 1 Filed 01/16/18 Page 1 of 82 Page ID #1

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the  
Central District of California

United States of America  
v.  
Yi-Chi Shih ("SHIH") and  
Kiet Ahn Mai ("MAI"),  
Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief:

(1) From an unknown date but no later than February 15, 2013, and continuing to October 19, 2015, in the County of Los Angeles in the Central District of California, defendants SHIH and MAI violated:

Code Section	Offense Description
18 U.S.C. § 371	Conspiracy

(2) And, on or about December 30, 2013, in the County of Los Angeles in the Central District of California, defendant SHIH violated:

Code Section	Offense Description
50 U.S.C. § 1705(a), 18 U.S.C. § 2	The International Emergency Economic Powers Act ("IEEPA")

This criminal complaint is by \_\_\_\_\_  
Please see attached \_\_\_\_\_  
☐ Continued on the \_\_\_\_\_

Sworn to before me and signed by \_\_\_\_\_  
Date: \_\_\_\_\_

City and state: Los Angeles, California Hon. Paul L. Abrams, U.S. Magistrate Judge  
Printed name and title

ARREST WARRANT/DETENTION



The background of the slide is a dark blue-grey collage. It features various financial data visualizations: a bar chart on the left, a line graph with an upward trend in the center, a pie chart on the right with segments labeled 35%, 15%, and 5%, and several other smaller charts and graphs at the bottom. A binary code pattern (0s and 1s) is overlaid across the entire background.

## GRANT AUDITS AND USE OF GRANT FUNDS

## GRANT AUDITS AND USE OF GRANT FUNDS

- NIH sent letters to approximately 60 institutions alleging scientists were diverting IP from NIH-supported research to foreign countries – led to **terminations**

ASIAN AMERICA

### Texas cancer center ousts 3 scientists over Chinese data theft concerns

The MD Anderson Cancer Center was among 55 medical research facilities contacted by the NIH over concerns of researchers' ties to foreign governments.



The University of Texas MD Anderson Cancer Center in Houston on Sept. 20, 2012.

Pat Sullivan / AP file

TIME

### Emory University Fires 2 Neuroscientists Accused of Hiding Chinese Ties

BY TARA LAW MAY 25, 2019

Emory University fired two neuroscientists after they were accused of failing to disclose foreign research funding and connections with China.



## FALSE CLAIMS ACT



## FALSE CLAIMS ACT

- First half of 2019: DOJ announced more than \$750 million in settlements
- Duke University: **\$112 Million** for submitting falsified research to NIH and EPA

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Monday, March 25, 2019

### **Duke University Agrees to Pay U.S. \$112.5 Million to Settle False Claims Act Allegations Related to Scientific Research Misconduct**

Duke University has agreed to pay the government \$112.5 million to resolve allegations that it violated the False Claims Act by submitting applications and progress reports that contained falsified research on federal grants to the National Institutes of Health (NIH) and to the Environmental Protection Agency (EPA), the Justice Department announced today.

*Thank You*

**BSF**

BOIES SCHILLER FLEXNER