



Research Security and Integrity

Eric Schweser (CTR)

DOE Counterintelligence Officer

27th Annual NSPAA Technical Assistance Workshop

June 2023



1. Research Security Background
2. Research Security Threat Examples
3. Research Security Risk Analysis
4. Research Security Best Practices
5. Research Security Resources
6. DOE Grant Fraud Risks
7. My Contact Information
8. Questions/Discussion

What is Research Security???

As stated by the NSPM-33 Implementation Guidance, research security is defined as **“safeguarding the research enterprise against the misappropriation of research and development to the detriment of national or economic security, related violations of research integrity, and foreign government interference.”**

1. NSDD-189 – National Security Decision Directive 189 (NSDD-189) (Sep 1985)

- National Policy on the Transfer of Scientific, Technical, and Engineering Information
- NSDD-189 remains a cornerstone of the fundamental research enterprise, making a clear distinction between fundamental and classified research and stating that **products of fundamental research should remain “remain unrestricted” to the “maximum extent possible.”**

[NSDD-189 Link Click Here](#)

2. JASON/NSF – JASON Report on Fundamental Research Security (Dec 2019)

- “NSF charged JASON to produce an unclassified report that can be widely disseminated and discussed in the academic community, providing technical or other data about specific security concerns in a classified appendix.”
- Of the 6 questions NSF charged JASON to answer relevant to openness in fundamental research, principles of scientific openness, areas of fundamental research necessitating more control, controls on information, and best practices researchers can put in place, this report details “the results from the ensuing inquiry, discussions, and debates engaged with NSF, senior university administrators, the intelligence community, law enforcement, and others.”

[**JASON Report Click Here**](#)

[**NSF Response to JASON Report Click Here**](#)

3. AAU/APLU/COGR – University Actions to Address Concerns about Security Threats and Undue Foreign Government Influence on Campus (May 2020)
 - “APLU and AAU have previously identified and shared effective practices universities are employing to **ensure the security of research, protect against intellectual property theft and academic espionage, and prevent actions or activities by foreign governments and/or other entities that seek to exert undue foreign government influence or infringe on core academic values** (e.g. free speech, scientific integrity, etc.)...

[AAU/APLU/COGR Report Click Here](#)

3. AAU/APLU/COGR – University Actions to Address Concerns about Security Threats and Undue Foreign Government Influence on Campus (May 2020)

- Effective practices:
 1. Awareness Building and Communications
 2. Coordination, Training of Faculty and Students
 3. Regular Interactions with Federal Security and Intelligence Agencies
 4. Protection of Data and Cybersecurity
 5. Protection of Intellectual Property and Use of Technology Control Plans
 6. Review of Collaborations, Contracts, and Foreign Gifts
 7. Reviewing, Updating, and Enforcing Conflict of Interest Policies
 8. Foreign Travel Safeguards and Protections
 9. International Visitors to Campus
 10. Export Control Compliance

[**AAU/APLU/COGR Report Click Here**](#)

4. NSF – Webpage on NSTC Research Security Subcommittee, NSPM-33 Implementation Guidance Disclosure Requirements & Standardization

- “The National Science and Technology Council (NSTC) Research Security Subcommittee has worked to **develop consistent disclosure requirements** for use by senior personnel, as well as to develop proposed common disclosure forms for the Biographical Sketch and Current and Pending (Other) Support sections of an application for Federal research and development (R&D) grants or cooperative agreements. NSF has agreed to serve as steward for these common forms as well as for posting and maintenance of the table entitled, NSPM-33 Implementation Guidance Pre- and Post-award Disclosures Relating to the Biographical Sketch and Current and Pending (Other) Support.” This website provides up-to-date information on disclosure requirements.

[**NSF Webpage on NSPM-33 Implementation Guidance Click Here**](#)

3. NSF – Webpage on NSTC Research Security Subcommittee, NSPM-33 Implementation Guidance **Disclosure Requirements** & Standardization



NSPM-33 Implementation Guidance

Pre- and Post-award Disclosures Relating to the Biographical Sketch and Current and Pending Support¹

Note: Where there are activities specific to the mission of the agency, this document may be modified by the Federal Research Funding Agency to address these disclosure requirements

September 1, 2022

Table Key

◆ = for new support only

◆ = If undisclosed at the time of application submission

Type of Activity	Biographical Sketch	Current & Pending Support	Facilities, Equipment & Other Resources	Project Reports	Post-Award Information Term & Condition	Disclosure Not Required
Professional Preparation (e.g., education and training)	✓					
Academic, professional ² or institutional appointments and positions, whether or not remuneration is received, and, whether full-time, part-time, or voluntary	✓					

[**NSF Webpage on NSPM-33 Implementation Guidance Click Here**](#)

NSPM-33 Implementation Guidance
Pre- and Post-award Disclosures Relating to the Biographical Sketch and Current and Pending Support
September 01, 2022

Type of Activity	Biographical Sketch	Current & Pending Support	Facilities, Equipment & Other Resources	Project Reports	Post-Award Information Term & Condition	Disclosure Not Required
All projects (including this project) currently under consideration from whatever source, and all ongoing projects, irrespective of whether support is provided through the proposing organization, another organization or <i>directly</i> to the individual and regardless of whether or not they have monetary value (e.g., even if the support received are in-kind contributions such as office/laboratory space, equipment, supplies, or employees)		✓		✓*	✓♦	
In-kind contributions that support the research activity for use on the project/proposal being proposed			✓			
In-kind contributions not intended for use on the project/proposal being proposed and have an associated time commitment		✓		✓*	✓♦	
Recently completed support or support that has ended						✓

NSPM-33 Implementation Guidance
Pre- and Post-award Disclosures Relating to the Biographical Sketch and Current and Pending Support
September 01, 2022

Type of Activity	Biographical Sketch	Current & Pending Support	Facilities, Equipment & Other Resources	Project Reports	Post-Award Information Term & Condition	Disclosure Not Required
Current or pending participation in, or applications to, programs sponsored by foreign governments, instrumentalities, or entities, including foreign government-sponsored talent recruitment programs		✓ Appropriate placement may be contract dependent)	✓ Appropriate placement may be contract dependent)	✓	✓	
Postdoctoral scholars, students, or visiting scholars who are supported by an external entity, and whose research activities are intended for use on the project/proposal being proposed			✓			
Postdoctoral scholars, students, or visiting scholars who are supported by an external entity, whose research activities are not intended for use on the project/proposal being proposed and have an associated time commitment		✓		✓*	✓♦	
Consulting that is considered part of an individual's appointment/agreement with their home organization and consistent with the proposing organization's "Outside Activities" policies and procedures						✓

NSPM-33 Implementation Guidance
Pre- and Post-award Disclosures Relating to the Biographical Sketch and Current and Pending Support
September 01, 2022

Type of Activity	Biographical Sketch	Current & Pending Support	Facilities, Equipment & Other Resources	Project Reports	Post-Award Information Term & Condition	Disclosure Not Required
Consulting that falls outside of an individual's appointment/agreement		✓		✓*	✓♦	
Travel supported/paid by an external entity to attend a conference or workshop						✓
Travel supported/paid by an external entity to perform research activities with an associated time commitment		✓		✓*	✓♦	
Honoraria or other given for the purpose of conferring distinction or to symbolize respect, esteem, or admiration unrelated to research oversight, supervision, or co-authorship						✓
Teaching commitments						✓
Startup company based on organization-licensed Intellectual Property (IP)						✓
Startup company based on non-organization-licensed IP		✓		✓*	✓♦	
Organizational startup packages provided to the individual from the proposing organization						✓

NSPM-33 Implementation Guidance
Pre- and Post-award Disclosures Relating to the Biographical Sketch and Current and Pending Support
September 01, 2022

Type of Activity	Biographical Sketch	Current & Pending Support	Facilities, Equipment & Other Resources	Project Reports	Post-Award Information Term & Condition	Disclosure Not Required
Startup packages from other than the proposing organization		✓		✓*	✓♦	
Unrestricted Gifts ³						✓
Training awards and prizes						✓
Mentoring as part of appointment or agreement, or mentor/mentee arrangements that do not involve the individual's research activities						✓
Academic Year Salary or salary provided to the individual by the home organization						✓
Core facilities and/or shared equipment that is broadly available						✓
F&A Reimbursement provide to the proposing/home organization						✓

5. COGR – Matrix of Science & Security Laws, Regulations, and Policies (Sep 2022)

- “COGR has developed a comprehensive chart that summarizes and compares federal laws, regulations, and policies in the area of science and security. The chart is divided into three separate tabs that cover (a) major federal-wide legislation or policy (e.g., National Presidential Security Memorandum 33, CHIPS and Science Act of 2022); (b) agency disclosure requirements for researchers and research institutions; and (c) agency conflict of interest policies.

COGR

An Association of Research Institutions

**COGR MEMBER PORTAL
LOGIN**

HOME ABOUT MEETINGS POLICY ISSUES RESOURCES CONTACT

COGR Matrix of Science & Security Laws, Regulations, and Policies

COGR has developed a comprehensive chart that summarizes and compares federal laws, regulations, and policies in the area of science and security. The chart is divided into three separate tabs that cover (a) major federal-wide legislation or policy (e.g., National Presidential Security Memorandum 33, CHIPS and Science Act of 2022); (b) agency disclosure requirements for researchers and research institutions; and (c) agency conflict of interest policies. The chart will be updated as new laws, policy and guidance are published. This new chart supersedes the matrix released in September 2021 (V.1), but continues to be accessible below for reference purposes only.

For questions regarding the comparison chart please contact Kris West (kwest@cogr.edu) or Krystal Toups (ktoups@cogr.edu).

[Excel Download \(V.2, Released 9/7/22\)](#)

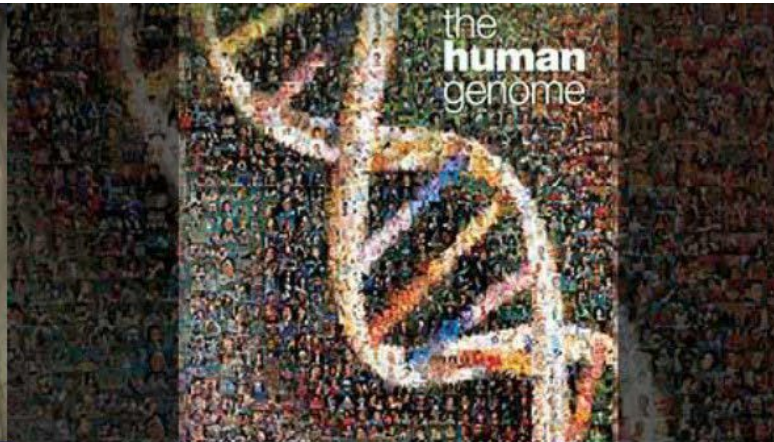
ARCHIVED: [Excel Download \(V.1, Released 9/2/2021\)](#)

[COGR Webpage Click Here](#)

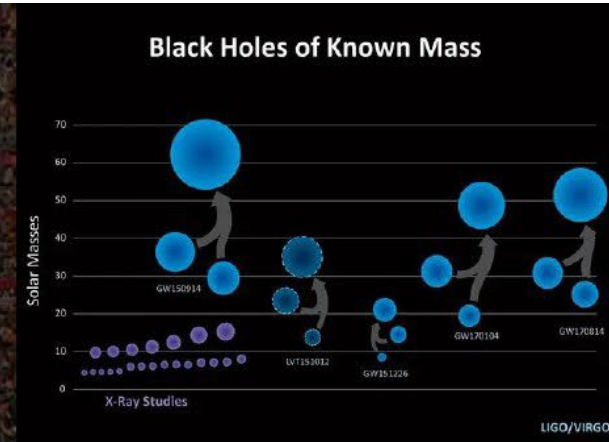
International research collaboration can provide valuable scientific breakthroughs....



European Organization for Nuclear Research
(CERN)



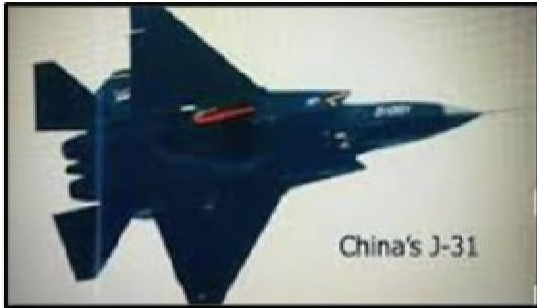
International Human Genome
Sequencing Consortium



Laser Interferometer Gravitational-
Wave Observatory (LIGO)

....but some research can and will be targeted for information collection, exploitation and unwanted technology transfer

These are NOT cooperative R&D efforts:



China's J-31



U.S F-35



Russia's A-50



U.S. E-3C



U.S. Reaper



China's Yilong-1

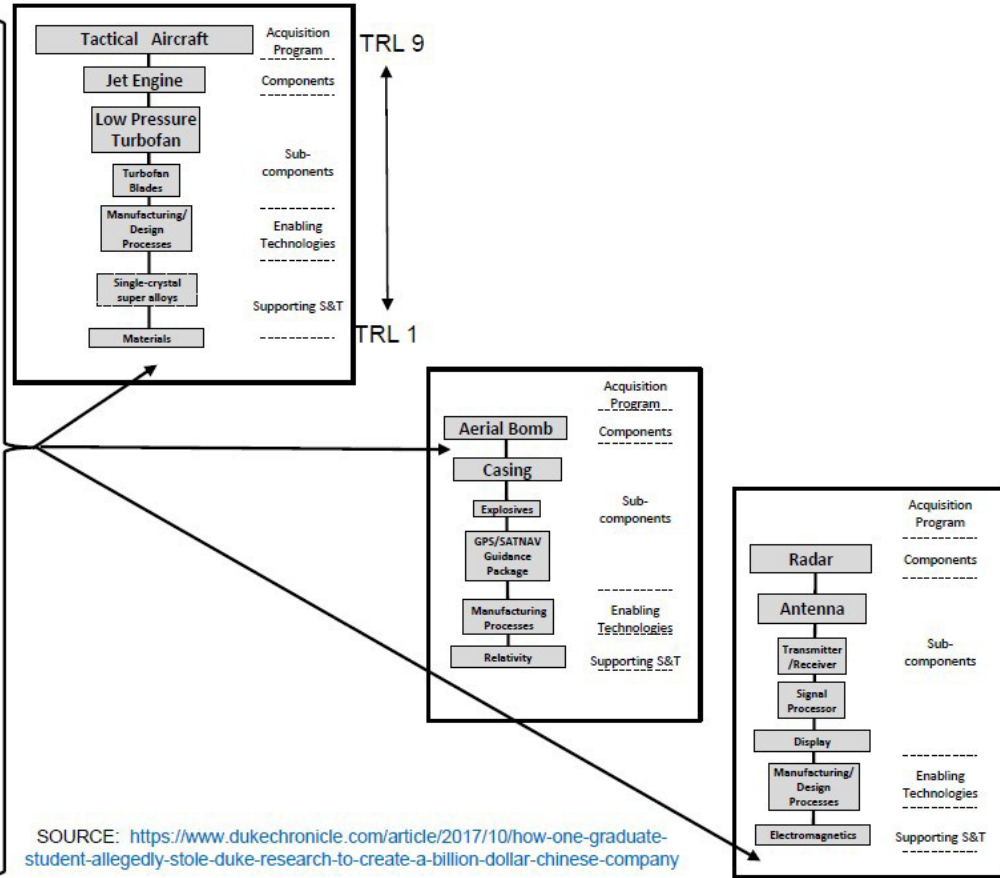


U.S. HUMVEE



China's Dongfeng EQ2050

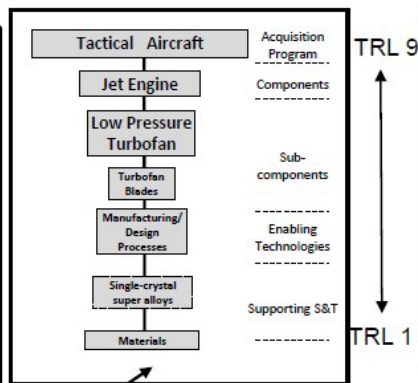
Tactical Aircraft Technology Decomposition Example



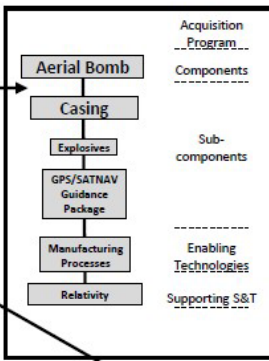
Tactical Aircraft Technology Decomposition Example



Tactical Aircraft Technology Decomposition Example

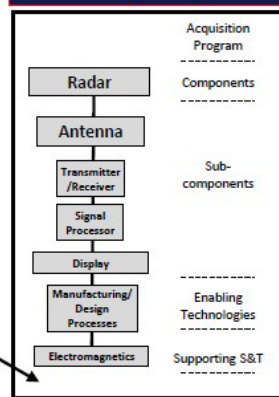


- Duke PI published in 2006 prototype of “invisibility cloak” to conceal objects from microwave detection (Air Force Office of Scientific Research funded)
- Ruopeg Liu joined the lab as a PhD student in 2006; initiated collaboration with a Chinese research lab, 2009 co-published new and improved version
- Unknown to Duke faculty, Liu allegedly began sending intellectual property and research information to the Chinese lab. FBI never charged Liu.
- Liu returned to China; in 2010 founded and served as President of Kuang-Chi Institute of Advanced Technology, now a multi-billion dollar conglomerate



IMPACT:

- Duke lost licensing, patents, and royalties
- China gained “invisibility cloak” technology to make fighter jets harder to detect

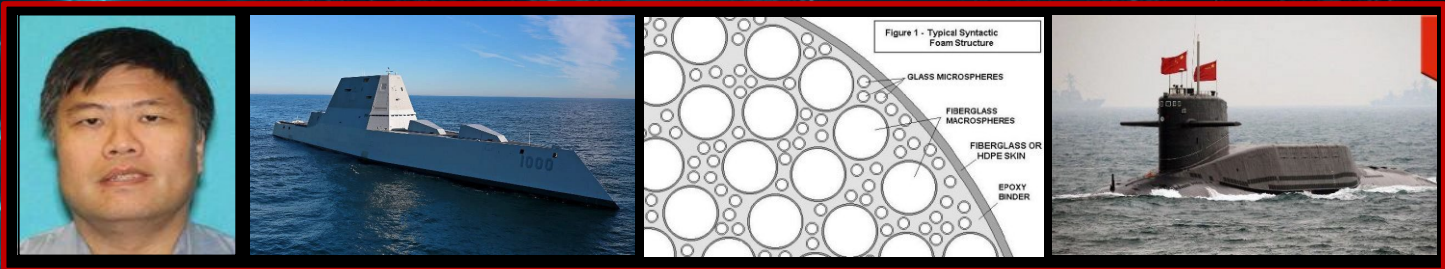


SOURCE: <https://www.dukechronicle.com/article/2017/10/how-one-graduate-student-allegedly-stole-duke-research-to-create-a-billion-dollar-chinese-company>

UNCLASSIFIED



SHAN SHI INSIDER THREAT CASE EXAMPLE



UNCLASSIFIED

How Does Technology Transfer by Insiders Work?

China Tech Transfer Vectors

- Multiple vectors used simultaneously to obtain key western technology identified in China's Five Year Plans.
- Funded and supported by Chinese Government at all levels.
- Case Example shows five of these vectors in action.



INTRODUCTION

U.S. vs Shan Shi summary

- Sophisticated Chinese Government Economic Espionage
- Sought to steal critical U.S. syntactic foam manufacturing technology
- First economic espionage prosecution in District of Columbia
- 7 individuals and 2 companies indicted
- 4 guilty pleas and 1 trial conviction

2 Charged With Espionage In Chinese Trade Secrets Theft

Houston man convicted of stealing trade secrets for China

July 30, 2019

HoustonPress



shombreadsenegor/flickr

Houston-Area Engineers Accused of Stealing Trade Secrets to Benefit Chinese Military

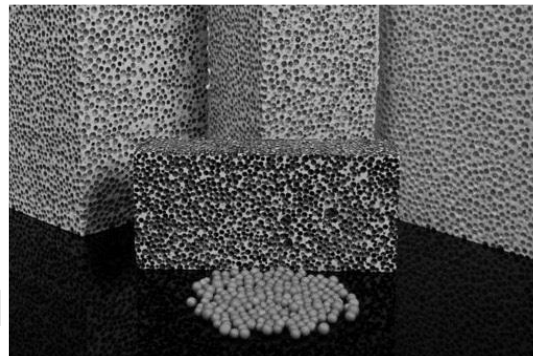
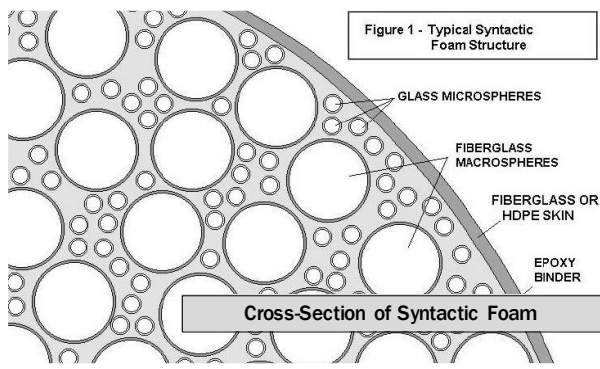


BREAKING NEWS
HEDWIG VILLAGE HOME AT CENTER OF INTERNATIONAL ESPIONAGE CASE

SYNTACTIC FOAM

Why Is It Important?

- Export-controlled: Provides key military and economic advantage
- Used in submarines, naval ships, and oil platforms
- \$2-20 billion industry in oil and gas
- China cannot make high-quality syntactic foam
- Took victim company Trelleborg over 40 years and millions of dollars to develop



CHINA'S FIVE-YEAR PLANS

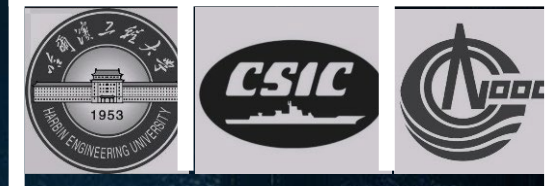


Why Does China Want Syntactic Foam?

- The 12th Five-Year Plan focuses on marine power
- Chinese Government Ministry of Information and Industry Technology (MIIT) names syntactic foam as a priority on "Made in 2025" list and sets aside \$70M
- CSIC, CNOOC, Harbin Engineering University form China Buoyancy Materials in 2013
- CBMF fails to create syntactic foam, HEU turns to economic espionage



CBMF Website



海洋工程装备科研项目

建议书

项目名称: 高性能深水浮力材料研制及典型海洋工程部件
应用技术研究

申报单位: 哈尔滨工程大学

参研单位: 深圳海油工程水下技术有限公司

台州中浮新材料科技股份有限公司

中海石油深海开发有限公司

中国船舶重工集团公司第七〇五研究所

项目负责人: 乔英杰 13351881930

研制周期: 2014年1月—2016年12月

编制日期: 2013年5月30日

工业和信息化部 财政部

CBMF, HEU, CSIC, CNOOC Contact

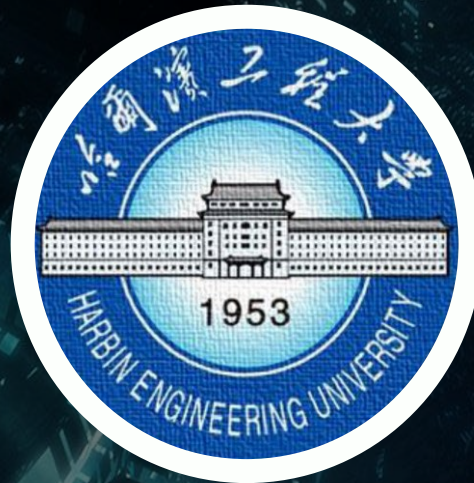
THE SCHEME

Stealing the Formula from the United States

- CBMF hires Harbin professor Shan Shi in 2014
- Shi was also a professor at Texas A&M
- China Buoyancy Materials becomes Create Better Materials
- Shi incorporates CBMI in Houston and receives \$3M from China



Shan Shi
CBMI
 President



THE CONTRACT

Stealing the Formula from the United States



- CBMF Contract with Shi



Shi- Party A

其它

事宜, 各方可进一步协商并订立补充协议或变更本协议与本协议具有同等法律效力。

方签字盖章后即生效。本协议一式柒份, 各方各执壹份存档。

1. Party A's Obligations and Responsibilities:

(1) Party A, through his own knowledge, capability and the relevant technology that he masters, actively brings in cutting-edge knowledge and high-level talented people, trains and raises the level of the design ability of CBM-Future and sets up a design team for CBM-Future.

(4) responsible for the coordination with local government and relevant departments to earnestly receive preferential policies from the government for Party A and also to actively work with Party A in the applications related to the "Thousand Talents Program" at the provincial level and at the national level and the 500 Elites Plan of Taizhou City, etc.;

THOUSAND TALENTS

Stealing the Formula from the United States



- Shi's Thousand Talents Application

Since I have over 20-year experiences in design and engineering of marine engineering field in U.S. and taking into consideration the situational reality in relation to our country's current implementation of the "Ocean Power" strategy, it is the right timing to return to the country for repaying with my services. I believe that I can make corresponding contributions to the development of our country's marine engineering endeavor and the advancement of technology of related marine engineering industries.

[3] Carry on, based on Taizhou CBM-Future New Material Science and Technology Co., Ltd., the structural design, material design and process design of the buoyance materials for drilling riser, and introduce and digest/absorb the relevant, critical U.S. technology and build China's first deepsea drilling buoyance material production line to satisfy the needs of our country's marine engineering development.

THEFT OF TRADE SECRETS

- Subjects create “targeting packages” of Trelleborg employees who work on syntactic foam using LinkedIn, recruit two Trelleborg employees
- Steal numerous trade secrets on macrosphere production, despite strict access controls at the company
- Send trade secrets to CBMF, which still fails to make syntactic foam but copies a key sub-component: macrosphere technology



Huang Hui
CBMF



Shan Shi
CBMI
President



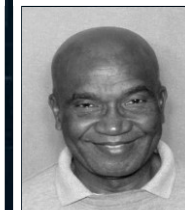
Gang Liu
Victim Co.



Kui Bo
CBMI VP



Oka Oche
Victim Co.



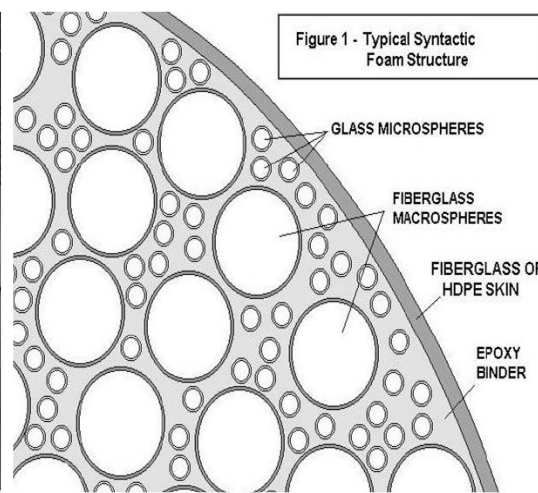
Sam Ogoe
Victim Co.



JW Randa
Victim Co.



CBMF Testing Facility in China

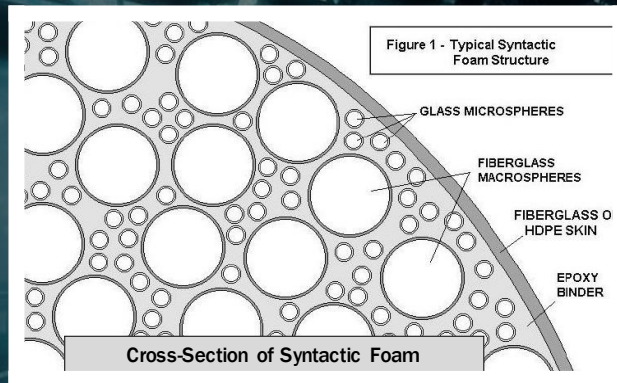


THE “BUSINESS PLAN”



Shi's Business Plan

- Shi offers to mass produce macrospheres for Trelleborg, using their own stolen technology.
- CBMF will offer joint venture to obtain rest of technology.
- CBMF will take over \$20 billion industry.
- CBMF will supply both Chinese military and civilian entities.
- Subjects say: “U.S. company will exit industry.”



Business Plan

CBM International, Inc.

Prospects of Military Applications of Solid Buoyancy Materials



UNDERCOVER OP

- May 23, 2017 - Undercover operation
- Bid on Lockheed proposal
- Provided list of projects for PLA Navy
- Arrests after presentation



CBM 中国未来 CBM INTERNATIONAL

Sales Record

Track Record						
No.	Customer	Project	Product / Service	Specifications	Contract Date	Notes
1	Hankin Engineering University (HEU), College of Shipbuilding and Ocean Engineering	NAV Research	Synthetic Foam	Water Depth: 1,000 meters; Density: 400 kg/m ³	Jul-14	
2	China National Offshore Oil Company (CNOOC), Designer Development Company		Synthetic Foam	Water Depth: 4,000 meters; Density: 320 kg/m ³	Feb-15	
3	China Shipbuilding Industry Corporation 725 Division		Synthetic Foam	Water Depth: 2,000 meters; Density: 500 kg/m ³	Apr-16	
4	China Shipbuilding Industry Corporation 710 Division		Synthetic Foam	Water Depth: 2,000 meters; Density: 500 kg/m ³	Mar-18	
5	Shenzhen Aerospace Lingang Group Co., Ltd.	Drone Research	Synthetic Foam	Density = 300 - 300 kg/m ³	Oct-18	
6	Chejiang Three Guimawa Intelligent Equipment Manufacturing Co., Ltd.	Sound & Acoustic Insulation	Synthetic Foam		Feb-16	
7	Trillaborg Offshore, US		Composite Hollow Microsphere	Water Depth = 8,000 Ft; Density = 440 kg/m ³	Apr-16	
8	SBM Offshore, US	Sea Water Intake Filter	Material Testing		Sep-16	
9	SBM Offshore, US	SCR Testing	Distructured Buoyancy Modules	Water Depth = 1,000 meters; Density = 400 kg/m ³	Dec-16	
10	China National Offshore Oil Company (CNOOC), Shenzhen Subsea Technology Company		DRM Repair		Feb-17	



Outcome



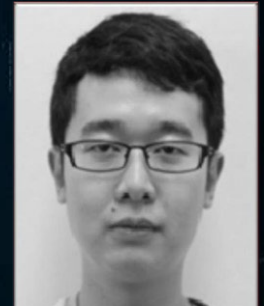
Shan Shi
Convicted at trial



JW Randall
Pleaded Guilty



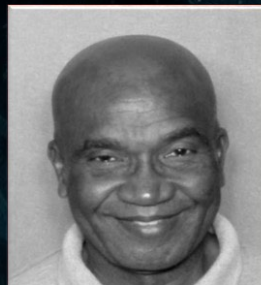
Uka Uche
Pleaded Guilty



Gang Liu
Fugitive



Kui Bo
Pleaded Guilty



Sam Ogoe
Pleaded Guilty



Huang Hui
Fugitive

UNCLASSIFIED

Technology Transfer Central to China's Development

"We should make use of the intellectual resources of other countries... We should not be reluctant to spend money on recruiting foreigners... It is a matter of strategic importance"

Deng Xiaoping, 1983

"In today's world S&T innovation has become critical for increasing comprehensive national strength... whoever holds the key to S&T innovation will be able to preempt the rivals and win the advantage..."

Xi Jinping, June 9, 2014



UNCLASSIFIED

Non-Traditional Collectors

UNCLASSIFIED

National Priorities

- National Development and Reform Commission
- Five-Year Plans
- Medium- and Long-Term Science and Technology Development Plan
- 16 Major Projects

Industry and Ministry Priorities

- Ministries
- Chinese Academy of Sciences
- State-Owned Enterprises
- Provincial and Municipal Governments

Incentives

- 1000 Talents Program
- 863/973 Programs
- Torch Plan
- Non-monetary incentives

Facilitation Platforms

- Consular Officials, especially S&Ts
- Professional and Cultural Organizations
- Companies with Government Ties
- Delegation Visits
- Joint Ventures/Acquisitions

Acquisition

- Co-opted Employees
- Hired Talent Under Contract
- Reverse Engineering
- Cyber Exfiltration

UNCLASSIFIED

Current Situation

China's Five-Year Plans For Worldwide Monopolies

New 13th Five-Year Plan National S&T Development Projects through 2030

Aircraft Engines and Gas Turbines	Brain Science and Artificial Intelligence	Smart-Grid Technology	New Materials
Big Data	Clean Coal	Intelligent Manufacturing and Robotics	National Cyberspace Security
Seed-Industry Innovation	Deep-Sea Space Station	Satellite Broadband Mobile Communications	Precision Medicine and Health Security
Quantum Communication and Computing	Deep-Space Exploration	Environmental Governance	

“The Chinese government is a company—disguised as a country--engaged in economic warfare.”

John Ferriola, Chairman and CEO, Nucor Corp, The Wall Street Journal, October 17, 2017

The Potential Cost

- We understand the Chinese Market is crucial but we want you to know that it will not be on a level playing field:
 - If your products are on the 13th Five Year Plan or Made in 2025 List, your company is a target
 - The goal of the Chinese Government is to create “monopolies”, which means eventually they want your company out of business.
 - The Chinese company you compete against or enter into a joint venture with has the full support of the Chinese Government and the tools of its security services and regulatory agencies at their disposal.
 - The Chinese company you compete against will have financial backing from the Chinese Government and will not have to make a profit.

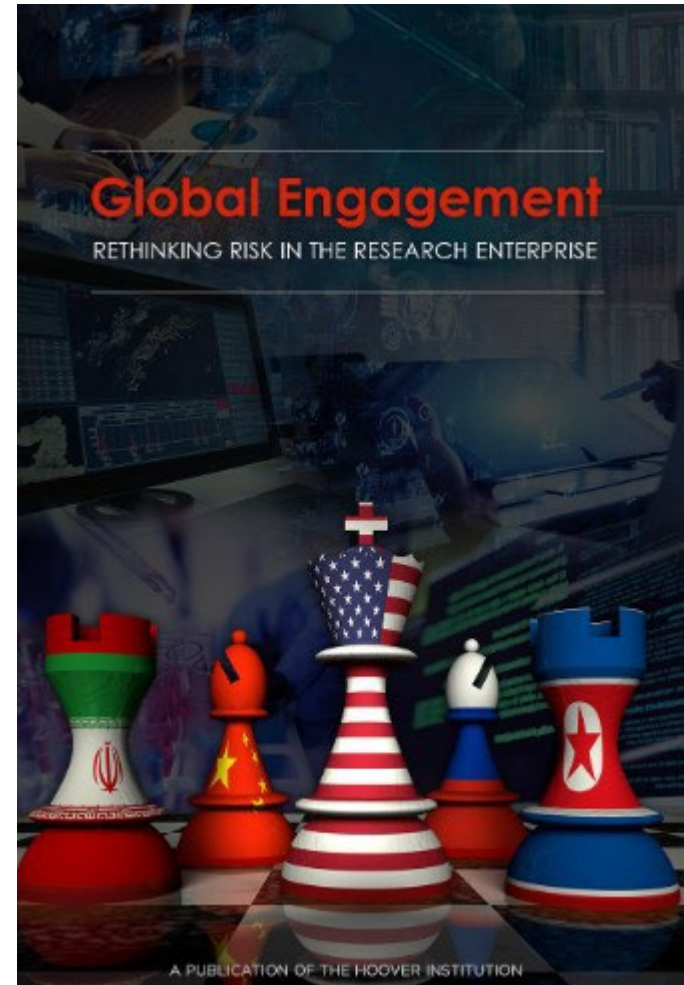
1. Hoover Institution's Global Engagement: Rethinking Risk in the Research Enterprise (July 2020)



[Global Engagement: Rethinking Risk in the Research Enterprise Webinar Link](#)

1. Hoover Institution's Global Engagement: Rethinking Risk in the Research Enterprise (July 2020)

The Hoover Institution's report *Global Engagement: Rethinking Risk in the Research Enterprise* documents collaborations between US and PRC scholars and research institutions that have directly contributed to the PRC's military modernization and argues that new approaches to identifying and managing foreign engagement risk are urgently required. The report includes an integrated program of policy recommendations that aim to reconcile America's commitment to open and globalized research with the imperative to safeguard US national security and economic competitiveness.



[**Global Engagement: Rethinking Risk in the Research Enterprise Link**](#)

1. NSTC – Recommended Practices for Strengthening the Security and Integrity of America’s Science and Technology Research Enterprise (Jan 2021)
 - “This document was developed by the Subcommittee on Research Security, in coordination with the National Security Council staff, and was reviewed by JCORE [the Joint Committee on the Research Environment]. The document outlines recommended guidelines for organizations that conduct research.”
 - The purpose of this document is to offer recommendations research organizations (e.g., universities, private companies, independent research institutes) can take to better protect the security and integrity of America’s research enterprise.
 - It serves as a complementary document to National Security Presidential Memorandum 33 (NSPM-33)

[NSTC Recommended Practices Click Here](#)

1. NSTC – Recommended Practices for Strengthening the Security and Integrity of America’s Science and Technology Research Enterprise (Jan 2021)
 1. Convey the importance of research security and integrity at the leadership level
 2. Ensure an organizational approach to research security
 3. Establish research security and integrity working groups and task forces
 4. Establish and operate a comprehensive research security program
 5. Establish and administer organizational policies regarding conflicts of interest, conflicts of commitment, and disclosure
 6. Require disclosure to the organization of all information necessary to identify and assess potential conflicts of interest and commitment
 7. Ensure compliance with Department of Homeland Security requirements for reporting foreign students and foreign researcher information.

[NSTC Recommended Practices Click Here](#)

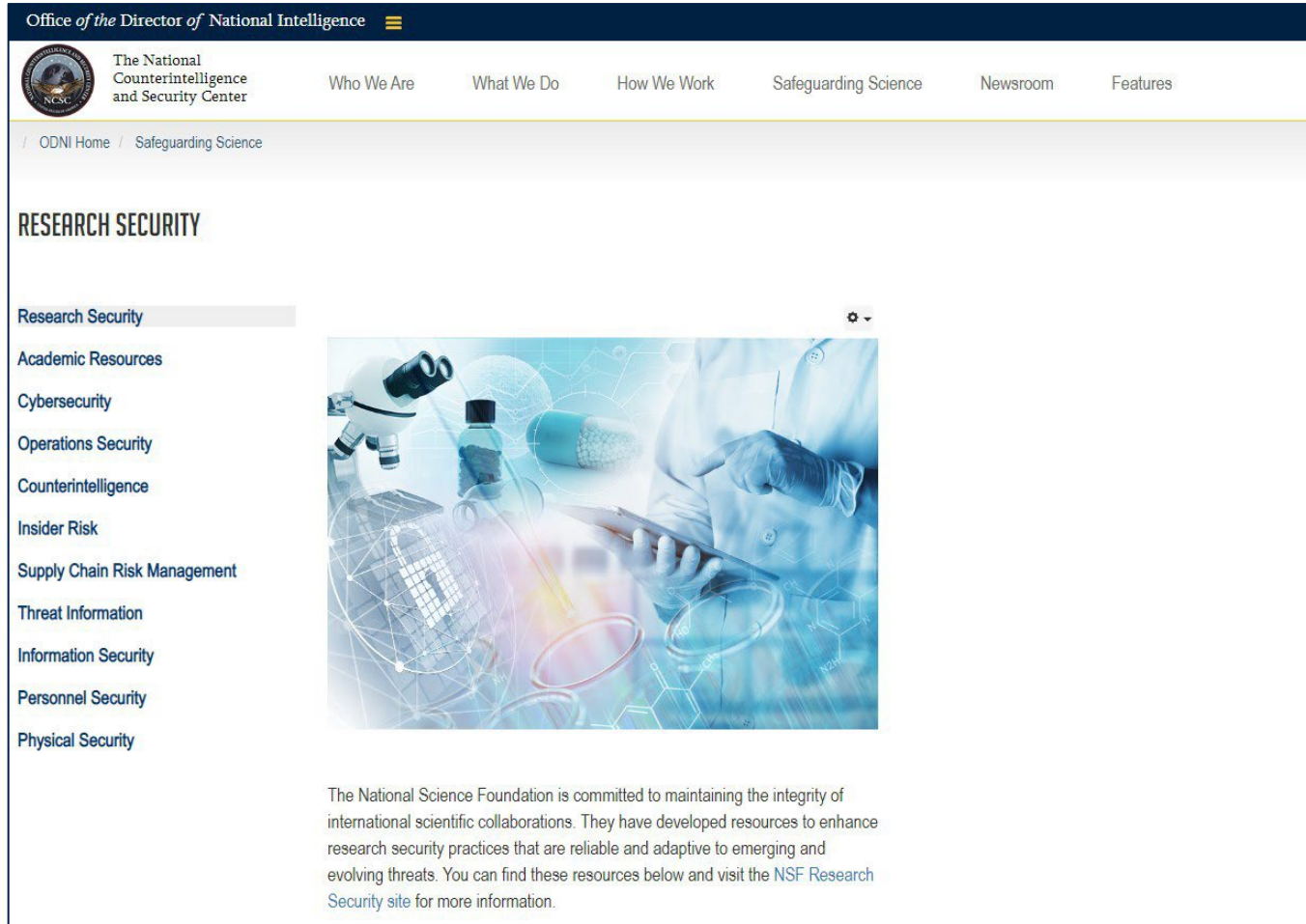
1. NSTC – Recommended Practices for Strengthening the Security and Integrity of America’s Science and Technology Research Enterprise (Jan 2021) (cont’d)
 8. Establish policies regarding digital persistent identifiers
 9. Ensure compliance with requirements for reporting foreign gifts and contracts
 10. Provide training to participants in the research enterprise on the responsible conduct of research
 11. Provide guidance for those considering participation in foreign government-sponsored talent recruitment programs
 12. Partner with local FBI field offices to strengthen research security
 13. Increase awareness of and protections against circumstances and behaviors that may indicate risk to research security and integrity
 14. Share information regarding potential violations of disclosure policies
 15. Establish and exercise effective means of discovering violations of disclosure policies and other activities that threaten research security and integrity

[NSTC Recommended Practices Click Here](#)

1. NSTC – Recommended Practices for Strengthening the Security and Integrity of America’s Science and Technology Research Enterprise (Jan 2021) (cont’d)
 16. Ensure appropriate and effective consequences for violation of disclosure requirements and engagement in other activities that threaten research security and integrity
 17. Include in employment agreements provisions that support research security and integrity
 18. Establish a centralized review and approval process for evaluating formal research partnerships.
 19. Establish and operate a risk-based security process for foreign travel review and guidance.
 20. Managing potential risks associated with foreign visitors and visiting scholars
 21. Establish and maintain effective data security measures

[NSTC Recommended Practices Click Here](#)

1. The National Counterintelligence and Security Center (NCSC) Research Security Website



Office of the Director of National Intelligence


The National Counterintelligence and Security Center

Who We Are | What We Do | How We Work | Safeguarding Science | Newsroom | Features

/ ODNI Home / Safeguarding Science

RESEARCH SECURITY

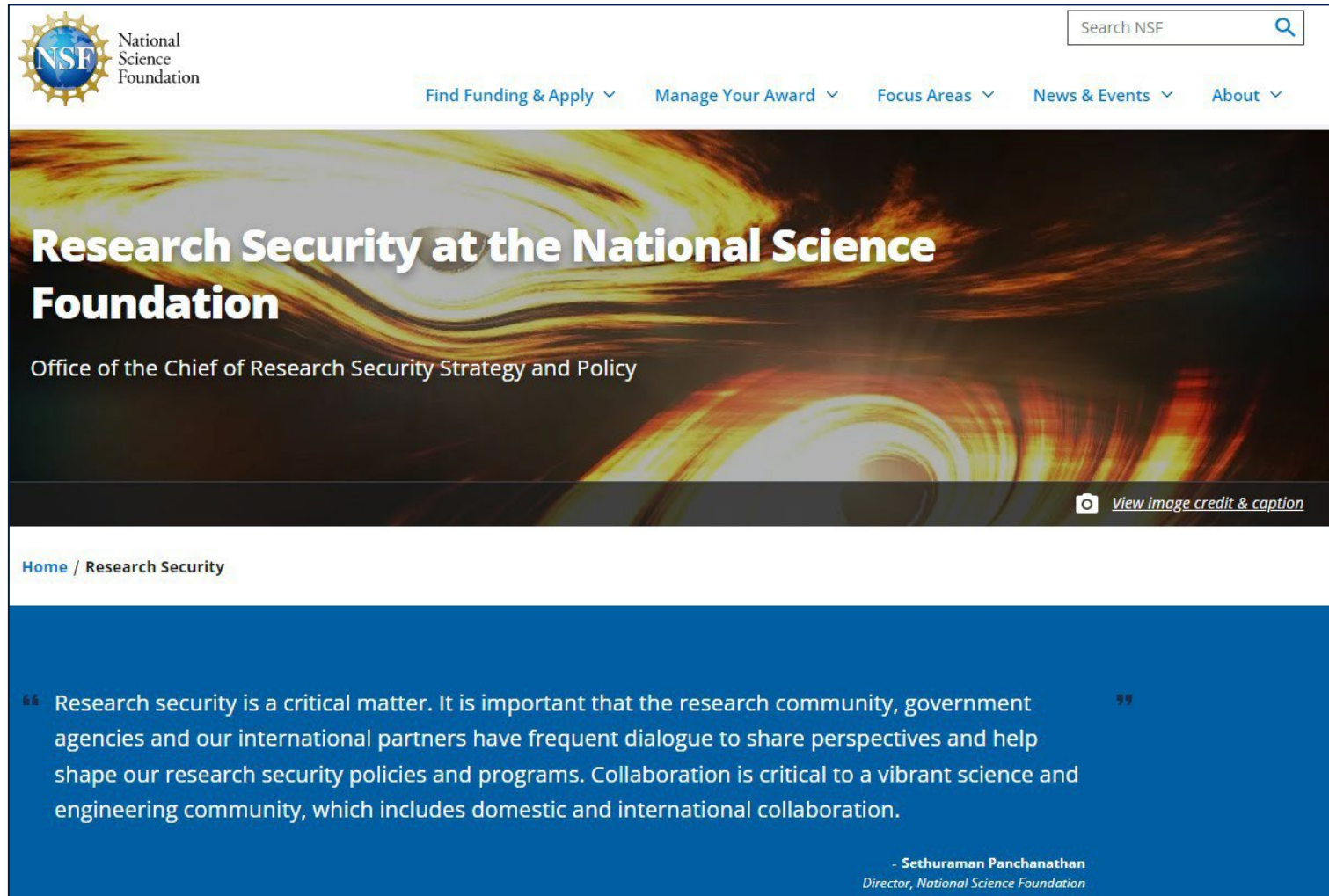
- Research Security
- Academic Resources
- Cybersecurity
- Operations Security
- Counterintelligence
- Insider Risk
- Supply Chain Risk Management
- Threat Information
- Information Security
- Personnel Security
- Physical Security



The National Science Foundation is committed to maintaining the integrity of international scientific collaborations. They have developed resources to enhance research security practices that are reliable and adaptive to emerging and evolving threats. You can find these resources below and visit the NSF Research Security site for more information.

NCSC Research Security Website

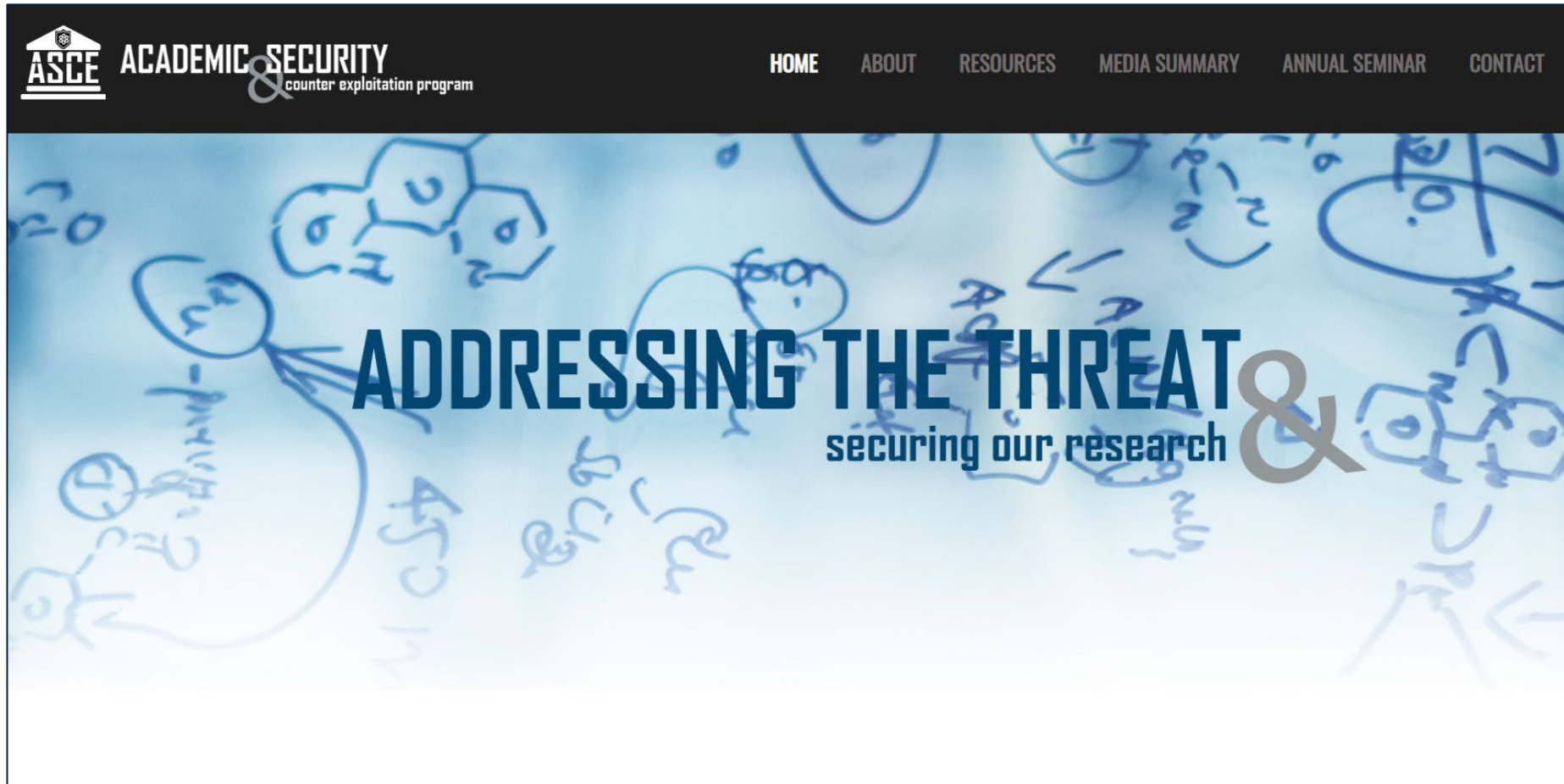
2. National Science Foundation (NSF) Research Security Website



The screenshot shows the NSF Research Security website. At the top left is the NSF logo. To its right is a search bar labeled "Search NSF". Below the logo and search bar is a navigation menu with the following items: "Find Funding & Apply", "Manage Your Award", "Focus Areas", "News & Events", and "About". The main header features a large, abstract image of a galaxy or nebula with the text "Research Security at the National Science Foundation" in large white font. Below this is the text "Office of the Chief of Research Security Strategy and Policy". A small icon and the text "View image credit & caption" are located at the bottom right of the header image. Below the header is a breadcrumb trail: "Home / Research Security". The main content area has a blue background with a quote: "Research security is a critical matter. It is important that the research community, government agencies and our international partners have frequent dialogue to share perspectives and help shape our research security policies and programs. Collaboration is critical to a vibrant science and engineering community, which includes domestic and international collaboration." The quote is attributed to Sethuraman Panchanathan, Director, National Science Foundation.

NSF Research Security Website

3. Academic Security and Counter-Exploitation (ASCE) Program Website



[ASCE Website](#)

3. Academic Security and Counter-Exploitation (ASCE) Program Website

BENEFITS OF JOINING ASCE

Join now and gain access to these benefits.



NETWORK

Access to the Academic Security & Counter Exploitation Portal on the Homeland Security Information Network



LISTSERV

Access to the Academic Security & Counter Exploitation Listserv



RESOURCES

Access to publication of EFFECTIVE PRACTICES related to countering the threats



TRAINING

Support for academic institutions to promote security and limit undue influence on institutions and personnel



CONNECTIONS

Participation in the annual Academic Security & Counter Exploitation Conference

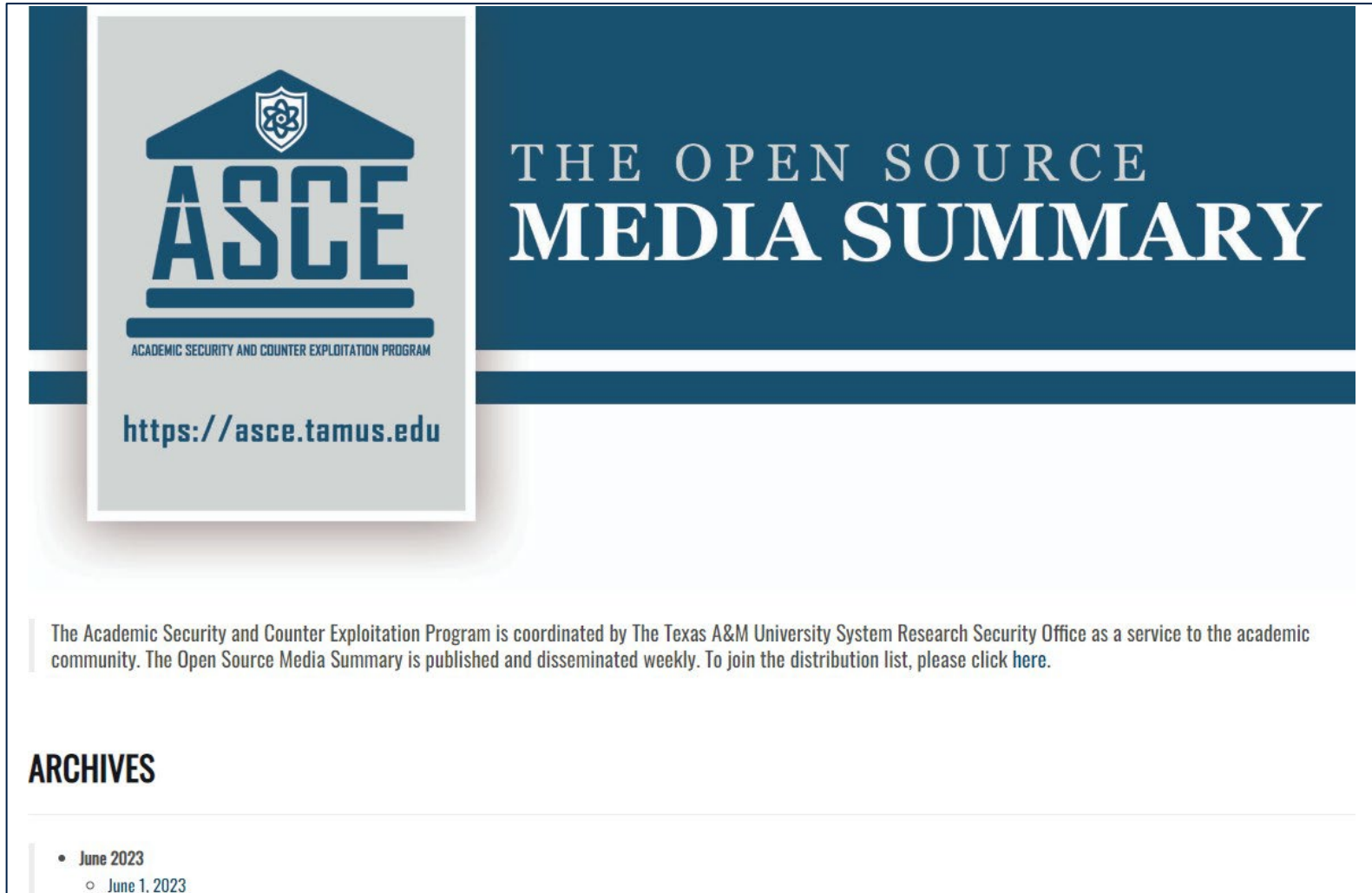


NEWSLETTER

Receipt of quarterly Academic Security Newsletter

[ASCE Website](#)

3. ASCE Media Summary Website



The screenshot displays the ASCE Media Summary Website. On the left, there is a logo for ASCE (Academic Security and Counter Exploitation Program) featuring a shield with a gear and a star above the letters 'ASCE'. Below the logo, the text 'ACADEMIC SECURITY AND COUNTER EXPLOITATION PROGRAM' is visible, followed by the URL <https://asce.tamus.edu>. On the right, a dark blue banner contains the text 'THE OPEN SOURCE MEDIA SUMMARY' in white, bold, uppercase letters. Below the banner, a paragraph of text reads: 'The Academic Security and Counter Exploitation Program is coordinated by The Texas A&M University System Research Security Office as a service to the academic community. The Open Source Media Summary is published and disseminated weekly. To join the distribution list, please click here.' Below this text is a section titled 'ARCHIVES' with a list of dates: 'June 2023' and 'June 1, 2023'.

[ASCE Media Summary Website](https://asce.tamus.edu)

3. ASCE Media Summary Website



**THE OPEN SOURCE
MEDIA SUMMARY**

<https://asce.tamus.edu>

June 1, 2023

**RESEARCH THEFT: THE TOUGHEST JOB OF SAFEGUARDING
UNIVERSITIES**

Nathan M. Greenfield | University World News | May 6, 2023

The memo titled "Guidance on Contact with CSIS [Canadian Security Intelligence Service]" sent by the University of Waterloo (UW) in southwestern Ontario, Canada, to its researchers at the end of March alarmed David Robinson, executive director of the Canadian Association of University Teachers. While the memo did not indicate which disciplines CSIS was interested in, the euphemism "high-priority research" was understood to mean science, technology, engineering and mathematics (STEM) fields. CSIS agents, the memo states, "may be concerned that you could be the target of a foreign state or entity, or they may have questions about some aspects of your activities". But the memo makes clear: "You do not have a legal obligation to talk to a CSIS officer"; you are not required to "speak with the officer immediately, or at the place where they approached you. If agents appear at your place of residence, you can ask them to reschedule the meeting to your workplace." After helpfully urging researchers to "remain calm, polite and ... truthful" in their statements, the memo ends by asserting the university's rights: "You must not consent to a search of University of Waterloo property without authorisation from the University of Waterloo."

Read the full article [here](#).

ASCE Media Summary Website

4. FBI China: The Risk to Academia



FEDERAL BUREAU OF INVESTIGATION

CHINA: THE RISK TO ACADEMIA

As of March 2018, more than 1.4 million international students and professors were participating in America's open and collaborative academic environment. The inclusion of these international scholars at U.S. colleges and universities entails both substantial benefit—and notable risk. Many of these visitors contribute to the impressive successes and achievements enjoyed by these institutions, which produce advanced research, cutting-edge technology, and insightful scholarship. However, this open environment also puts academia at risk for exploitation by foreign actors who do not follow our rules or share our values.

The vast majority of the 1.4 million international scholars on U.S. campuses pose no threat to their host institutions, fellow classmates, or research fields. On the contrary, these international visitors represent valuable contributors to their campuses' achievements, providing financial benefits, diversity of ideas, sought expertise, and opportunities for cross-cultural exchange. Any research institution hoping to be—and to remain—among the best in the world must attract and retain the best people in the world, wherever they are from. The FBI recognizes, and values, this unique package of benefits these international students and professors provide.

However, some foreign actors, particularly foreign state adversaries, seek to illicitly or illegitimately acquire U.S. academic research and information to advance their scientific, economic, and military development goals. By doing so, they can save their countries significant time, money, and resources while achieving generational advances in technology. Through their exploitative efforts, they reduce U.S. competitiveness and deprive victimized parties of revenue and credit for their work. Foreign adversaries' acquisition efforts can come in many forms, including overt theft, plagiarism, elicitation, and the commercialization of early-stage collaborative research.

The annual cost to the U.S. economy of counterfeit goods, pirated software, and theft of trade secrets is \$225–\$600 BILLION

FBI China: The Risk to Academia

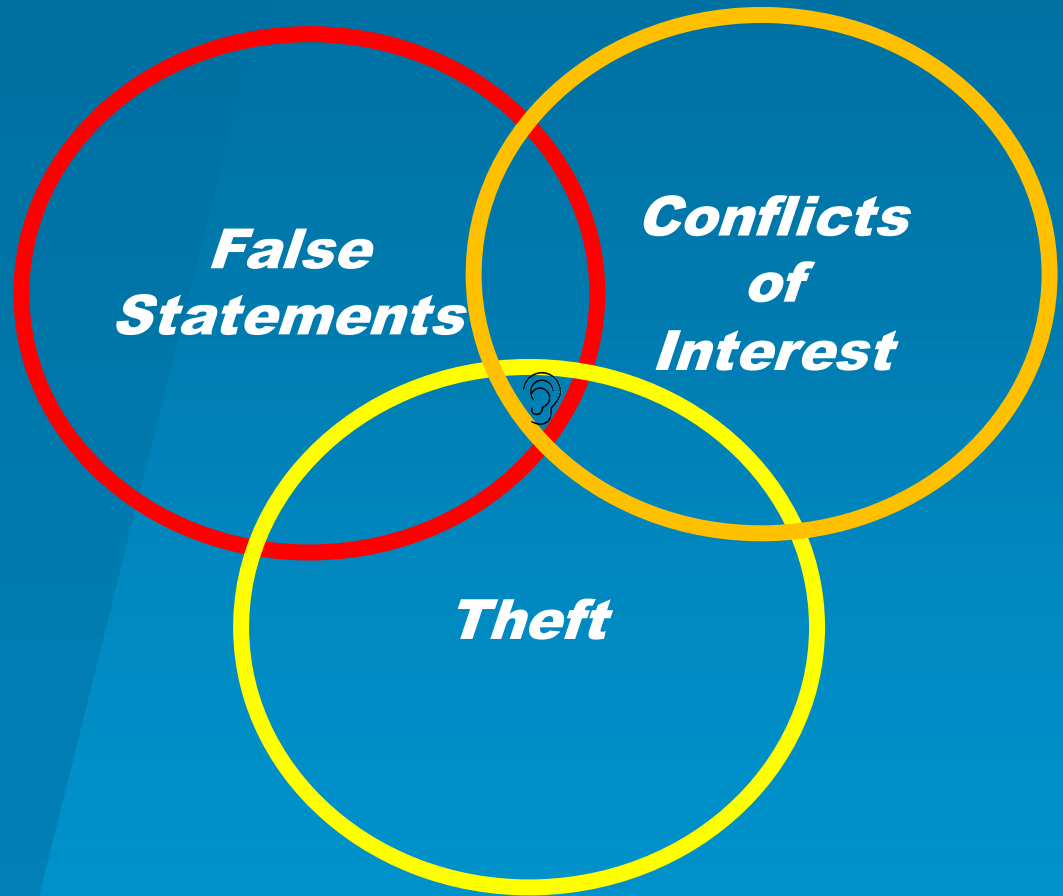
Grant Fraud Risks

Department of Energy Office of Inspector General



U.S. DEPARTMENT OF
ENERGY

Grant Fraud Risks



Some of the Many Common Grant Terms and Conditions and Other Promises

- Use award funds as promised
- Have and maintain an adequate accounting system
- Comply with civil rights and environmental laws
- Comply with cost share agreements
- Disclose foreign influence and other current and pending support
- Have and enforce conflict of interest policies and disclosure requirements
- Have and follow a procurement process
- Maintain and make books and records available for audit and inspection
- Accurately calculate and apply indirect cost rates
- Abide by the Buy America Act and Davis Bacon Act
- Follow the grantor agency financial and programmatic guides
- Not earn or keep a profit
- Comply with the Single Audit Act
- Notify grantor of changes in key personnel
- Conduct and document background checks on employees and volunteers
- Honor intellectual property rights
- Follow human and animal research protocols
- Obey research misconduct reporting obligations
- File financial and narrative progress reports as required
- Properly award and monitor subawards
- Submit reimbursement/ draw down claims for only allowable, allocable, and reasonable costs
- Follow salary cap policies
- Comply with mandatory disclosure rules
- Comply with "Never Contract with the Enemy" provisions

2 CFR § 200.113

Mandatory Disclosures

“The non-Federal entity or applicant for a Federal award must disclose, in a timely manner, in writing to the Federal awarding agency or pass-through entity all violations of Federal criminal law involving fraud, bribery, or gratuity violations potentially affecting the Federal award”

Failure to make required disclosures can result in suspension and debarment or other administrative actions.

Source: [5 CFR Part 200.113](#)

Red Flags of Potential Grant Fraud

- Complaints or tips from other funding agencies, recipient employees, ex-employees, competing recipients, or others.
- Poor or nonexistent recipient internal controls.
- Evidence of undisclosed related party transactions.
- Illogical or unsupported use of consultants or other vendors.
- Anticompetitive practices by suppliers and other vendors.
- Recipients who are unresponsive to requests for supporting documentation or other information, or who appear to not be making expected programmatic progress.

Red Flags of Potential Grant Fraud

- Illogical draw down patterns.
- Significant findings in a Single Audit Act, OIG, or other audit report.
- Anomalies or other information related to the integrity of a recipient employee or recipient agency.
- High turnover of recipient programmatic or financial staff.
- Inconsistent or inaccurate financial reports or narrative progress reports or updates.
- Recipients that lack the capacity, knowledge, or background to properly manage funds or their programs.

What Can You Do to Help?

- Be alert for indicators of potential fraud, waste, and abuse.
- Exercise professional skepticism. Document and follow-up on anomalies and red flags.
- Communicate any concerns about potential fraud, waste, and abuse with the OIG.

Reporting Suspected Fraud, Waste or Abuse:



Phone: (800) 541-1625 or (202) 586-4073

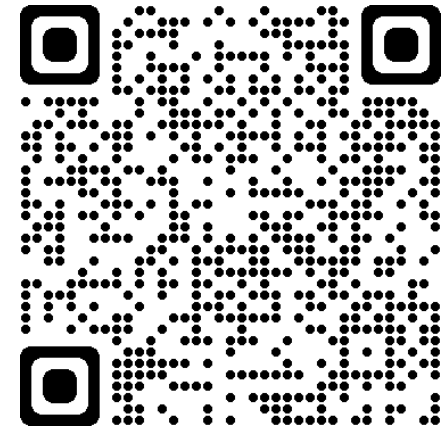


Email: ig hotline@hq.doe.gov



Postal Mail: U.S. Department of Energy
Office of Inspector General

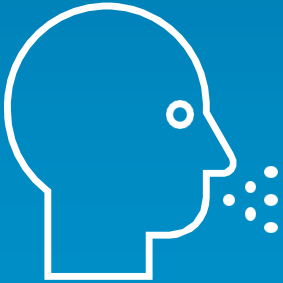
ATTN: Hotline
1000 Independence Avenue, SW
Mail Stop 5A-235
Washington, DC 20585



IG Hotline Website

<https://www.energy.gov/ig/ig-hotline>

Fraud Awareness Briefings



- The OIG is available to help educate DOE program staff, grantees and other stakeholders about grant fraud, contract fraud, and other compliance risks.
- Fraud prevention and early detection are key in saving taxpayer dollars and maximizing the likelihood of program success.

Fraud Risks

Ken Dieffenbach
Deputy Assistant Inspector General for Investigations
Department of Energy Office of Inspector General



U.S. DEPARTMENT OF
ENERGY

Reference Slides and Case Examples

Inducement Fraud

Two individuals were each sentenced to over 13 years in prison related to a conspiracy to submit research grant proposals using the stolen identities of real people to create false endorsements. The subjects also lied about their facilities, costs, the principal investigator on some of the projects, and other matters. Several agencies, including DOE were victims.

(Source: [Press Release, U.S. Attorney's Office, Middle District of Florida, September 11, 2015](#))

Overlapping Funding

The University of California paid a \$499,700 civil settlement to resolve allegations that it failed to disclose duplicative and overlapping funding from NSF and DOE awards and submitted progress reports to DOE which outlined work accomplished using NSF funds, among other allegations.

[\(Source: Press Release, U.S. Attorney's Office, Eastern District of California, December 11, 2014\)](#)

Sub Award Self Dealing / Corruption

An elected state official directed a federal grant subaward to a university while also separately negotiating with the university for a job to run the newly created program. He was sentenced to 114 months incarceration for bribery and extortion.

(Source: [Press Release, U.S. Attorney's Office, Eastern District of Virginia, August 12, 2011](#))

Theft

A former manager at an Illinois Community Action Agency stole over \$300,000 of DOE weatherization funding by submitting fraudulent invoices. The manager then diverted the funds for personal use. He was sentenced to 41 months imprisonment, ordered to pay \$431,828 in restitution, and was debarred for 3 years.

(Source: [DOE OIG Semiannual Report for period ending September 30, 2020](#) Page 31)

Organizational Self Dealing

Several individuals diverted federal grant funds intended for nonprofit public health services to for-profit entities controlled by the conspirators.

One individual was sentenced to 18 years in prison and ordered to pay \$13.5 Million in restitution.

(Source: [Press Release, U.S. Attorney's Office, Northern District of Alabama, June 17, 2016](#))

Research Security

The Van Andel Research Institute paid a \$5.5 M. civil settlement to resolve allegations that in a December 2018 letter, they made certain factual representations to HHS with deliberate ignorance or reckless disregard for the truth regarding foreign influence matters.

(Source: [Press Release, U.S. Attorney's Office, Western District of Michigan, December 19, 2019](#))

Counterintelligence Officer (CIO) Eric Schweser (CTR)

Email: eric.schweser@srs.gov

Phone: 803-507-0419

DOE Office of Intelligence and Counterintelligence
Savannah River Field Office
Aiken, SC

OSTP NSPM 33 Email: ResearchSecurity@ostp.eop.gov

Questions/Discussion