SRA INTERNATIONAL | SOCIETY OF RESEARCH ADMINISTRATORS INTERNATIONAL

Extensive New Foreign Disclosure Obligations and Security Requirements: How to Comply With the NSPM-33 and SBIR/STTR Updates

Edward T. Waters

Mindy B. Pava

FELDESMAN TUCKER LEIFER FIDELL LLP

PRESENTER: EDWARD “TED” WATERS

Contact Information:

Ewaters@ftlf.com
(202) 466-8960

- Well known for his expertise in federal grants, government reimbursement systems, cost accounting and administrative issues, and his strategic handling of organizations facing crises, Ted has been counsel to numerous organizations in the non-profit sector in the past 25+ years.
- Ted has been Managing Partner of Feldesman Tucker since 2003. He has represented clients in front of federal and State courts, legislative bodies, administrative tribunals, Offices of Inspector General and federal agencies.
- Ted leads trainings for an equally diverse array of organizations both state, regional and national associations as well as individual clients.
- Ted is a member of the National Grants Management Association (NGMA) and is also a member of the National Association of College and University Attorneys (NACUA).

SRA INTERNATIONAL

PRESENTER: MINDY B. PAVA

Contact Information:

MPava@ftlf.com
(202) 466-8960

- Mindy serves as counsel in the firm's Litigation and Investigations, Federal Grants and Health Care and Education practice groups.
- Mindy's practice focuses on helping federal grantees as they navigate all facets of agency and/or judicial review. She is a seasoned litigator who represents federal grant recipients, including research institutions, health centers, and Head Start programs, when dispute resolution needs arise.
- In addition to Mindy's work in federal and state courts, she represents organizations in responding to civil investigative demands and subpoenas. Mindy also advises clients on how to mitigate compliance risk through internal investigations.

DISCLAIMER

Portions of these materials have been prepared by the attorneys of Feldesman Tucker Leifer Fidell LLP. **The opinions expressed in these materials are solely their views and not necessarily the views of Feldesman Tucker Leifer Fidell LLP.**

The materials are being issued with the understanding that the authors are not engaged in rendering legal or other professional services. **If legal assistance or other expert assistance is required, the services of a competent professional with knowledge of your specific circumstances should be sought.**

COPYRIGHT NOTICE OF ORIGINAL MATERIALS

- These slides are being made available to you and your organization as a participant of an FTLF presentation. You are ONLY permitted to duplicate, reproduce and/or distribute these materials within your organization.
- Note: a membership organization may not consider its members to be "within the organization" for purposes of sharing materials.
- **These slides may not be otherwise photocopied, reproduced, duplicated, and/or distributed outside your organization and/or posted on a website without prior written permission from the authors.**
- Any other use or disclosure is a violation of federal copyright law and is punishable by the imposition of substantial fines.
- Copyright is claimed in all original material, including but not limited to these slides and other resources or handouts provided in connection to this training, exclusive of any materials from federal laws and regulations and any documents published by the federal government.

AGENDA

1. Research Security: Background and Overview
2. NSPM-33 Implementation
3. SBIR/STTR Foreign Disclosure Updates
4. If You Remember Anything from This Talk…

1. Research Security: Background and Overview

SHOW ME THE MONEY

- In FY2021, the U.S. Government supplied $49 billion in R&D funding to U.S. institutions of higher education (55% of all R&D spending in higher ed).
- Of that federal contribution, the Department of Defense supplied $7.4 billion (15 percent) of all such federal research funding.
- Important for institutions to update and modify award application management processes and research security procedures to be in line with federal expectations.

RESEARCH SECURITY AND INTEGRITY: OSTP MISSION

- Director of the Office of Science and Technology Policy shall: "establish or designate an interagency working group to coordinate activities to protect federally funded research and development from foreign interference, cyber attacks, theft or espionage and to develop common definitions and best practices for federal science agencies and grantees, while accounting for the importance of the open exchange of ideas and international talent required for scientific progression and American leadership in science and technology."

-- Language from National Defense Authorization Act of 2020 (Public Law 116-92, Sec. 1746(a)).

OSTP KEY PRIORITIES

1. Protecting America's security and openness;
2. Being clear in delivery of guidance and information to impacted communities, so compliance is straightforward and minimally burdensome; and
3. Ensuring that federal government policies do not fuel xenophobia or prejudice.

-- Guidance for Implementing National Security Presidential Memorandum-33 (NSPM-33) on National Security Strategy for U.S. Gov't-Supported Research and Development (Jan. 4, 2022)

A CAUTIONARY TALE

- (September 2023): False Claims Act complaint filed in E.D. Pa. unsealed against Penn State, alleging that the university defrauded the government by falsely certifying its cybersecurity compliance. (Lawsuit originally filed Oct. 2022).
- Defense contractors must follow 22 detailed requirements from the National Institute for Standards and Technology for protecting controlled unclassified information that span digital and physical protections, as well as audits and proper security configurations.
- Alleged that Penn State provided self-attestations of compliance to DoD as required, but that the self-attestations were false.
- Allegations of (i) missing records for certain university projects in a database used monitor contractor performance and (ii) use of a commercial version of Microsoft 365 OneDrive, which was not certified, for cloud services.

SRA INTERNATIONAL

A CAUTIONARY TALE

- Who was the whistleblower? The former Chief Information Officer for Penn State's Applied Research Laboratory. Whistleblower alleges that PSU disregarded some of his recommendations relating to compliance and may have left controlled unclassified information exposed.
- The lawsuit details the whistleblower's steps to investigate his concerns and alleges that the false certification concerns were repeatedly presented to university leadership and ignored.
- Demonstrates the new focus of enforcement agencies in pursuing cybersecurity-related fraud by grant recipients.
- Demonstrates the importance of self-attestations to compliance with research security procedures.
- **The take-away: universities should brace for additional scrutiny (and potential claims) in this area.**

SRA INTERNATIONAL

2. NSPM-33 Implementation

NSPM-33 BACKGROUND

- National Security Presidential Memorandum-33, signed by Trump in January 2021, directs federal agencies to standardize requirements for federal research support relating to disclosure of conflicts of interest and conflicts of commitment to mitigate the risks of undue foreign influence on such research activity.
- Under the Biden Administration, White House Office of Science and Technology Policy ("OSTP") has continued implementation of NSPM-33 across the federal government.

REQUIREMENTS FROM NSPM-33

- Research organizations receiving more than $50 million in federal science and engineering funding for two consecutive years must certify that they have in place certain research security standards in the following four areas:
  - Cybersecurity;
  - Foreign travel security;
  - Research security training; and
  - Export control training.

THE KEY TEXT

- **Risk Identification and Analysis**… "Heads of funding agencies shall require that research institutions receiving federal science and engineering support in excess of $50 million dollars per year certify to the funding agency that the institution has established and operates a research security program. Institutional research security programs should include elements of **cyber security, foreign travel security, insider threat awareness and identification, and, as appropriate, export control training**."

-- NSPM-33 Section 4(g) relating to "Risk Identification and Analysis."

DRAFT STANDARD REQUIREMENT: SEEKING UNIFORMITY IN IMPLEMENTATION

- A draft Research Security Programs Standard Requirement was been created by OSTP, together with Federal agencies and the Office of Management and Budget, to ensure that there is uniformity across Federal research agencies in implementation.
- Published in Federal Register in March 2023; public comments sought and received until June 2023.
- If draft Standard Requirement is approved, covered research organizations have until early 2024 to establish a research security program that complies with the OSTP standards.

THOSE RESEARCH SECURITY STANDARDS WOULD INCLUDE…

- Certification of maintaining a research security program meeting the requirements (self-certification on SAM.gov);
- Establishment of international travel policies for covered individuals engaged in federally-funded R&D traveling for business, teaching, conference attendance and research purposes, or who receive offers of sponsored travel;
- Implementation of research security training, tailored to appropriate personnel and students;
- Implementation of baseline safeguarding protocols and procedures for information systems used to store, transmit and conduct federally-funded R&D; and
- Providing training to relevant personnel on requirements and processes for reviewing foreign sponsors, collaborators and partnerships, if subject to export control restrictions.

ONE AGENCY EXAMPLE

- DoD issues "Policy for Risk-Based Security Reviews of Fundamental Research" on June 8, 2023. The policy directs DoD grantees to:
  - Implement new risk-based security review processes to standardize COI/COC disclosure requirements, including more frequent COI/COC disclosure or removal of PIs deemed to be security risks;
  - Provide more institutional supervision of foreign commitments or activities by PIs, along with clearer authorization for an institution to block certain commitments or activities deemed to pose undue security risks;
  - Consider if a proposed research collaboration may involve a "county of concern" or an institution on the sanctions list; and
  - Ensure that international research collaborations are not discouraged.

THE NEXT STEPS

- Many universities and organizations offered comments to the draft Standard Requirements during the public comment period, to ensure the needs and interests of university researchers were known to policymakers.
- Anticipated that federal government will issue greater specificity of the requirements in the implementation guidance in fall 2023.
- Until then, institutions of higher education are:
  - Establishing “Security Compliance Standing Committees” comprised of faculty and staff to facilitate the implementation of the requirements.
  - Tasking existing research compliance teams with working with other offices across the institute to prepare for anticipated changes in systems, policies and processes.

3. SBIR/STTR Foreign Disclosure Updates

HEIGHTENED DISCLOSURES ABOUT FOREIGN TIES

- Since the passage of the SBIR and STTR Extension Act of 2022, participating agencies have been required to collect information about applicants' foreign investments and affiliations. However, there was no uniform way to gather the information.
- **Effective May 3, 2023:**
  - The SBA has amended the Policy Directive of the SBIR and STTR programs to harmonize agencies' information collection. Participating agencies will use a "standard template form" to collect disclosures of foreign investment and affiliations of small business concerns applying to the SBIR and STTR programs.
  - The amendment permits participating agencies to require a certification to the accuracy and completeness of an applicant's responses – inaccurate or misleading disclosures may result in penalties including fines, being excluded from future grants, and even individual criminal liability.
  - Appendix III to the Policy Directive - provides agencies with a uniform method of assessing risky applicants based on foreign ties and investments.

DISCLOSURE QUESTIONS FOR COMPANIES SEEKING SBIR/STTR AWARDS

- Is any owner or covered individual of the awardee party to any malign foreign talent recruitment program?
- Is there a parent company, joint venture, or subsidiary, of the applicant that receives funding from, any foreign country of concern?
- Does the applicant have any current or pending contractual or financial obligation with an enterprise owned by a foreign state or any foreign entity?
- During the previous 5-year period, did the applicant have any technology licensing or intellectual property transfers to a foreign country of concern?
- Does the applicant have an owner, officer, or covered individual that has a foreign affiliation with a research institution located in a foreign country of concern?

See SBA, ***SBIR/STTR Policy Directive, App. III***, 88 Fed. Reg. 19704 (April 3, 2023), available at: https://www.federalregister.gov/documents/2023/04/03/2023-06870/small-business-innovation-research-program-and-small-business-technology-transfer-program-policy

IMPACT ON AWARDS

- The SBIR and STTR Extension Act of 2022 mandates that agencies will be required to establish and implement due diligence procedures to assess eligibility for SBIR and STTR awards based on security risks, no later than **June 27, 2023**. Agency due diligence procedures must:

  - Assess the cybersecurity practices, patent analysis, employee analysis, and foreign ownership of a small business concern seeking an award, including its financial ties and obligations to a foreign country or foreign entity; and

  - Assess awards and proposals or applications, using a risk-based approach as appropriate, including through open-source analysis and analytical tools, for the nondisclosure of information.

Denial of Awards: Agencies are prohibited from making a SBIR or STTR award if: (1) the small business has ties with a foreign country of concern; and (2) the agency determines that the ties pose a risk to national security.

IMPLEMENTATION OF THE NIH SBIR AND STTR FOREIGN DISCLOSURE REQUIREMENTS

- Prior to issuing an award, the NIH will determine whether the applicant: (1) has a covered individual that is a party to a malign foreign talent recruitment program; (2) has a business entity located in China or another foreign country of concern; and (3) has a covered individual with a foreign affiliation with a research institution located in China or another foreign country of concern.
- NIH will provide applicants with a chance to address any identified security risks prior to award. NIH will not issue an award if the risk cannot be resolved, but a finding of foreign affiliations DOES NOT necessarily disqualify an applicant.
- Post-award, recipients are responsible for monitoring their relationships with foreign countries of concern and must submit an updated disclosure form to report any changes or material misstatements that pose a risk to national security. Updated disclosure forms are required within 30 days of any change in ownership, entity structure, covered individual or other substantive change in circumstance.
- An applicant will be required to repay all funding amounts received under the award if: (1) it makes a material misstatement that NIH determines poses a risk to national security; and (2) there is a change in entity structure that the NIH determines poses a risk to national security.

-- See NIH Notice (June 16, 2023), 88 FR 39439.

SRA INTERNATIONAL

4. If You Remember Anything From This Talk . . .

ANY MISREPRESENTATION MATTERS

- Bio-Adhesive sentenced to pay $562,500 in restitution to NSF and $319,199 to the EPA (June 2021), after pleading guilty to two counts of making false statements in grant applications.
- Company applied for and received multiple STTR and SBIR grants from NSF and EPA from 2013-2016. The proposals contained misrepresentations regarding its eligibility to seek such awards, as well as other material aspects of the project (budget, employees, etc.).
- Examples: (1) A certain employee was eligible to the PI, with knowledge that he was not eligible; (2) a subcontract would be paid to North Carolina A&T University; and (3) an individual would act as chief technology officer, with knowledge that the individual had not agreed to do so.
- No fraudulent foreign disclosures, but still OIG investigation and findings of fraud in the SBIR Program.

- The recent focus on research security and foreign influence conflicts of interests further emphasizes the **<u>importance of disclosures</u>**.

2018 CASE STUDY

- Virginia Tech professor was found guilty of conspiring to commit federal grant fraud and making false statements (Sept. 2018).
- Professor Yiheng Zhang founded Cell-Free Bioinnovations, a research firm that relied on federal grant funding. Zhang also worked as a paid researcher for the Tianjin Institute of Industrial Biotechnology, Chinese Academy of Science, since 2014.
- In 2015, Zhang submitted grant proposals to NSF that were found to be fraudulent:
  - SBIR/STTR funds were to be used for research already done in China;
  - Intent to use grant funds for other projects, rather than the projects for which the funds were requested; and
  - Zhang intended to obstruct the investigation by submitting false timesheets.
- Sentence: Incarcerated for 3 months; home incarceration for 2 years.

SRA INTERNATIONAL

IN TODAY'S WORLD…

- Under the NPSM-33, Virginia Tech is a research organization receiving more than $50 million in federal science and engineering funding for two consecutive years. Would it certify that it had certain research security standards in place?
- Would Zhang's conduct have violated those research security standards?
- Under the new SBIR/STTR foreign disclosure requirements, did Zhang accurately disclose his ties to China and certify his response?
- Did the NSF use a uniform method of assessing risky applicants?
- *Where does the fault lie between Zhang, Virginia Tech and the NSF?*

QUESTIONS?

Edward T. Waters

ewaters@ftlf.com

Mindy B. Pava

MPava@ftlf.com

Feldesman Tucker Leifer Fidell LLP

(202) 466-8960 (Reception)

(855) 200-3822 (Training Team)