SRA INTERNATIONAL
ANNUAL MEETING
CHICAGO 2024
OCTOBER 26-30

Wading Through the Research Security Morass: New Standards, Enforcement Priorities, and Guidance During a Complex Time

By: Mindy B. Pava, Esq.
Rosie Dawn Griffin, Esq.
FELDESMAN LEIFER LLP

Presenter: Mindy B. Pava

Contact information:
Mpava@Feldesman.com
202.466.8960

- Mindy Pava serves as Partner in the firm's Litigation and Investigations, Federal Grants and Health Care and Education practice groups.
- Her practice focuses on helping federal grantees as they navigate all facets of agency and/or judicial review or 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.

Presenter: Rosie Dawn Griffin

Contact information:
RGriffin@Feldesman.com
202.466.8960

- Rosie Dawn Griffin serves as Partner in the firm's Health Care, Litigation and Government Investigations, Government Contracts, and Federal Grants practice groups.
- She counsels and litigates on behalf of a diverse group of federal grant recipients. Rosie also defends clients facing investigations and litigation under the False Claims Act and similar statutes.
- She advises clients on compliance with regulatory and program requirements and assists clients in assessing fraud and compliance risk, including through internal investigations.

DISCLAIMER

These materials have been prepared by the attorneys of Feldesman Leifer LLP. **The opinions expressed in these materials are the views of Feldesman Leifer LLP and not necessarily the views of the federal government, any state government or of any other organization or person.**

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 a Feldesman Leifer LLP training program. You are ONLY permitted to duplicate, reproduce and/or distribute these materials in 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. **Long-Awaited White House OSTP Research Security Programs Guidelines:** What Does the Final Version Mean for You?
2. **Focus on Cybersecurity**
   - Enforcement Approach
   - Takeaways
3. **Focus on Foreign Travel Security**
   - Compliance Expectations and Scenarios
4. **Other Notable Research Security Changes**
   - NSF
   - Export Enforcement and Compliance Resources

1. OSTP Guidelines: Expectations vs. Reality

Guidelines for Research Security Programs at Covered Institutions

- On July 9, White House OSTP released long-awaited Guidelines
  - Intended to assist federal agencies in implementing certification requirements for "covered institutions" to ensure the institutions have research security programs (RSPs) addressing four areas.
- What is a "covered institution"?
  - An institution of higher education, federally funded research and development center or non-profit research institution; and
  - Receives more than $50 million per year (three-year average of R&D obligations).
- Guidelines "encourage" federal agencies to impose research security obligations for non-covered institutions

Guidelines for Research Security Programs at Covered Institutions

- Covered institutions will be required to certify that their RSPs address:
  - (i) cybersecurity
  - (ii) foreign travel security
  - (iii) research security training and
  - (iv) export control training.

- The Guidelines do not provide the specific certification language needed, which makes it difficult to address risk under the False Claims Act.

Guidelines for Research Security Programs at Covered Institutions

- **Implementation timeline:**
  - Within six months of promulgation, agencies must provide OSTP their plans to update their policies to reflect the new guidelines. (January 9, 2025).
  - Updated policies then take effect six months after that. (July 9, 2025).
  - Covered institutions have no more than 18 months after agency plans go into effect to comply.
- **Overall takeaway:** Assuming the schedule is not extended, these requirements cannot go into effect any sooner than end-of-year 2026 or early 2027.

Draft Policy vs. Final Guidance

- Final Guidelines give federal funding agencies and universities lots of discretion in exactly how to implement the policy.
- We envision you will be expanding existing research security protocols, rather than adopting wholesale changes.
- Draft proposal in February 2023 –less flexibility:
  - Certify compliance annually;
  - Publish security plans;
  - Designate a security "point of contact";
  - 9 topics that research security training needed to cover; and
  - Advance authorization of foreign travel by researchers.
- Final Guidelines removed prescriptive language, focused on broad principles. Many existing systems should be compliant.
- **Wild card:** variations in how different agencies interpret the guidelines.

How Will Researchers Be Impacted?

- Must undergo periodic security training – both for research projects and for work-related travel abroad.
- Universities must keep records of work-related travel abroad funded by government sponsors (but not of personal travel).
- Because agencies have flexibility to determine what projects and which researchers are covered, it's difficult to say how many researchers will be affected.

2. OSTP Guidelines: Focus Area 1 – Cybersecurity

Final Guidelines: Somewhat Unclear

- Institutions of higher education are required to "certify that the institution will implement a cybersecurity program consistent with the cybersecurity resource for research institutions described in the CHIPS and Science Act, within one year after the NIST of the Department of Commerce publishes that resource."
- NIST published an initial draft in August 2023 (Interagency Report 8481). The guidance document is written at a high-level and does not contain specific standards an institution can use to evaluate whether its existing cybersecurity controls are consistent with Final Guidelines.
- Covered institutions that are not IHE must comply with another NIST resource, or a resource maintained by another research agency (not clearly identified).
- Prior drafts of Guidelines: more specific, set forth cyber procedures that were consistent with FAR 52.204-21.

Should You Be Concerned About Unclear Cyber Requirements Guidance?

- Cybersecurity is a challenging area for many universities and research institutions.
- It is also a busy enforcement area and a priority for the Department of Justice, as reflected in DOJ's annual priorities and several recent False Claims Act settlements.

DOJ Enforcement Focus

- DOJ's **Civil Cyber-Fraud Initiative**, announced in October 2021, uses the False Claims Act to promote cybersecurity compliance by government contractors and grantees who "knowingly":
  - Provide deficient cybersecurity products or services.
  - Misrepresent their cybersecurity practices or protocols.
  - Violate obligations to monitor and report cybersecurity incidents and breaches.
- DOJ's CY 2024 enforcement priorities include holding contractors/grantees accountable for "knowing" violation of applicable cybersecurity requirements.
- We expect enforcement efforts to continue to ramp up.

DOJ Enforcement Focus

What's a "knowing" cybersecurity violation under the False Claims Act?

- [T]he terms "knowing" and "knowingly"—
  - mean that a person, with respect to information—
    - has actual knowledge of the information;
    - acts in deliberate ignorance of the truth or falsity of the information; or
    - acts in reckless disregard of the truth or falsity of the information; and
    - require no proof of specific intent to defraud.

Cyber Enforcement Example 1: Penn State

- October 2022, Penn State was sued by a former CIO for alleged false claims related to DoD contracts.
- Allegations:
  - Knowing failure to safeguard CUI as contractually required and submission of false security compliance reports.
- Obligation:
  - DFARS clause 252.204-7012 requires DoD contractors to provide “adequate security” to protect CUI—at minimum includes implementing NIST SP 800-171 security controls.
  - Clauses 252.204-7019 and -7020 require self-assessment and self-certification of compliance with NIST SP 800-171.

Cyber Enforcement Example 2: Georgia Tech

- July 2022, Georgia Tech Research Corporation sued by two whistleblowers for alleged false claims related to DoD contracts.
- February 2024, DOJ intervened.
  - First cybersecurity-related FCA intervention since DOJ unveiled the Civil Cyber-Fraud Initiative.
- Allegations:
  - Knowing failure to adhere to proper standards in processing and storing CUI.
  - Retaliation.
- Obligation:
  - DFARS hook to NIST SP 800-171 compliance, self-assessment, and self-certification.

Takeaways

- DOJ is actively pursuing noncompliance with cybersecurity requirements, including by encouraging whistleblowers to file suits for financial reward.
- False Claims Act risk extends beyond actual knowledge
  - Cybersecurity obligations are myriad and complex, but recipients of federal funds are expected to be on top of them;
  - Liability can attach to "turning a blind eye" to an issue, "sweeping problems under the rug," and "burying one's head in the sand" when confronted with a potential cybersecurity gap or failure.
- Violations must be "material" to trigger FCA liability.

Risk Mitigation

- IHEs and research institutions can mitigate risk of cybersecurity violations by:
  - Evaluating the accuracy of representations and certifications made to funding agencies.
  - Creating and retaining organized, contemporaneous documentation supporting the accuracy of representations/certifications.
  - Ensuring internal policies and procedures meet ongoing updates to regulatory requirements and industry best practices.
  - Encouraging internal whistleblowing through a robust reporting structure for any potential cybersecurity gaps or issues.

3. OSTP Guidelines: Focus Area 2 – Foreign Travel Security

Final Guidelines: Focus On Two Elements

1. **Covered institutions to offer training**
   - Covered institutions must certify that they will provide foreign travel security training to covered individuals who engage in international travel, described as including "sponsored international travel, for organizational business, teaching, conference attendance, or research purposes."
   - Covered individuals mean an individual who "contributes in a substantive, meaningful way to the scientific development or execution of a research and development project…" and "is designated as a covered individual by the federal research agency concerned."
   - OSTP states that it will, in coordination with other federal agencies, contract with a qualified entity to develop a training module for this purpose.
   - The training will be implemented within one year of a foreign travel security training resource being made available by a federal agency, and covered individuals will take the training at least one time every six years.

Final Guidelines: Focus On Two Elements

2. Covered institutions must report on travel records

- Covered institutions must implement a travel reporting program, which records international travel of covered individuals when traveling internationally for business, teaching, conferences, or other research purposes, if a federal research agency has determined that security risks warrant travel reporting in accordance with the covered individual's R&D award.
- Potential troublesome area:
  - Buy-in and support will be needed from researchers to use the required travel system and share travel records.
  - Institution will need to have a process for obtaining (and maintaining) the required records.

Foreign Travel Security: Key Questions

- How far does the scope of the "organization business" travel record requirement reach?
  - Does it include, for example, consulting work that may be outside of the individual's appointment but still constitutes business travel?
- How detailed should the records be?
  - Draft policy required covered institutions to establish international travel policies and procedures including, for example, mandatory security briefings, disclosure and authorization requirement, and electronic device security.

Foreign Travel Security: Group Discussion

- Scenario Number One: you're assisting your institution to implement a foreign travel reporting system.
  - How broadly does it apply?
  - What data elements do you want to capture?
  - What guidance do you provide for determining whether something is "personal" vs covered, research-related travel?
  - When do you require submission of this information?
  - What about last-minute travel?
  - What happens when someone forgets to report?
  - Are there any data elements or information you would require individuals to report after travel is complete?

Foreign Travel Security: Group Discussion

- Scenario Number Two: now flip the perspective—imagine you're subject to travel reporting requirements.
  - What is reasonable to require in terms of reporting?
    - Think in terms of both timing and content.
    - What about applicability?
  - What guidance would be helpful to you in determining whether something is "personal" vs covered, research-related travel?
    - Is it less burdensome to simply report all foreign travel? Too intrusive?
  - What would make you appreciate the importance of reporting?

4. Other Research Security Developments

Remaining OSTP Research Security Guidelines

3. Research Security Training

- Covered institutions must certify that they have implemented a research security training program that will be available to covered individuals and that will address their "unique needs, challenges, and risk profiles."
- Covered institutions also will have to certify that it ensures covered individuals take the required training in one of two ways:
  - Through use of NSF-developed training modules.
  - Through modules developed in-house or by a third party so long as the modules include specific examples of problematic behavior and stress global collaboration.

Remaining OSTP Research Security Guidelines

4. Export Control Training

- Covered individuals engaged in research and development work that involves export-controlled technology must complete export control and compliance training.
- Institution must certify that the training has been completed.
- Training is met by completion of Bureau of Industry and Security (BIS) trainings (or others) covering:
  - export control and compliance,
  - requirements and processes for reviewing foreign sponsors, collaborators and partnerships.

Another word on export control compliance..

- On August 14, Bureau of Industry and Security issued a press release regarding its initiatives related to compliance of export control laws—intended to put universities on notice of the importance of assessing their export control risks and compliance programs.
- New compliance note "details conduct commonly disclosed by academic institutions over the past ten years that constitutes export control violations." Goal—to develop "lessons learned."
- BIS also published a list of resources—export compliance tools, including informational and vetting resources, and recent enforcement examples.
- **The takeaway:** BIS is interested in educating the academic community regarding export compliance risks—but also will be holding institutions accountable for failing to implement compliance programs.

NSF's Foray into Research Security

- On July 24, NSF announced a five-year, $67 million investment to establish SECURE (Safeguarding the Entire Community of the U.S. Research Ecosystem).
- $50 million to University of Washington, $17 million to Texas A&M.
- The NSF SECURE Center: clearinghouse for information to help the research community identify and mitigate foreign interference risks by sharing reports, providing training, and strengthening ties between funding agencies and the research community.
- The SECURE Center will have five regional centers managed by six institutes of higher education (Northeast, Southeast, Midwest, Southwest, West).
- SECURE Analytics: support the analytics needs of the research community with enhanced expertise in landscape analyses, risk modeling and data reporting.

FELDESMAN

Rosie Dawn Griffin

Rgriffin@feldesman.com

Mindy B. Pava

Mpava@feldesman.com

SRA INTERNATIONAL