NIH Current and Pending Other Support (CPOS) and Research Security Training Requirements

I. PURPOSE AND BACKGROUND

This policy provides institutional guidance on reporting **Current Pending Other Support (CPOS)** to the National Institutes of Health (NIH). NIH requires Other Support disclosures for all individuals designated as **Senior/Key Personnel** on grant applications.

The NIH Grants Policy Statement defines Senior/Key Personnel as:

"The PD/PI and other individuals who contribute to the scientific development or execution of a project in a substantive, measurable way, whether or not they receive salaries or compensation under the grant. Typically, these individuals have doctoral or professional degrees. Senior/Key personnel must devote measurable effort to the project whether or not salaries or compensation are requested. 'Zero percent' effort or 'as needed' are not acceptable levels of involvement for those designated as Senior/Key Personnel."

Effective **October 1, 2025,** Senior/Key Personnel must complete training on CPOS disclosure requirements, as outlined in NIH Guide Notice NOT-OD-25-133.

As recipients of NIH funding, **PAVIR** is committed to full compliance with federal requirements. While this policy focuses on NIH, Investigators should be aware that other sponsors may have similar disclosure requirements. PAVIR expects compliance with all applicable sponsor policies.

II. POLICY

A. NIH CPOS Reporting Requirements

Accurate preparation and disclosure of CPOS is a critical responsibility of **Principal Investigators (PIs)** and **Key Personnel**. NIH typically requires an updated CPOS form at the following stages:

- **Just-in-Time (JIT)**
- **Annual Research Performance Progress Reports (RPPR)**
- **As needed, when new support arises during the project period**

PAVIR requires timely and accurate disclosure of all resources made available to a researcher in support of and/or related to any and all of their research endeavors, regardless of whether or not they have monetary value and regardless of whether or not they are based at the institution the researcher identifies for the current grant. This includes but is not limited to the following:

1. External Funding Sources

- Federal (e.g., NIH, DoD)
- State (e.g., TRDRP)
- Non-federal (e.g., foundations, societies)
- Industry-sponsored agreements (e.g. via CRADA)

2. Internal Awards

- Competitive institutional grants (e.g., pilot awards)

3. In-Kind Contributions

- Lab space, equipment, supplies, personnel
- High-value resources not freely available (e.g., unique cell lines)

4. Consulting Activities

- If involving research activities

5. Monetary Donations

- Monetary donations given to institutions or directly to senior/key personnel that support research activities related to an individual are given with an expectation, and therefore, such donations must be reported as other support

Other support does *not* include training awards, prizes, start-up support from the US based institution, or gifts.

For **foreign resources**, NIH requires documentation (e.g., contracts, agreements, appointment letters) and translations, if not in English.

B. Responsibilities of PIs and Key Personnel

- Disclose new sources of Other Support to PAVIR immediately upon awareness
- Collaborate with PAVIR Contracts and Grants team to determine NIH reporting obligations
- Participate in the preparation and attestation of CPOS documentation
- Complete Research Security Training

Failure to comply with the above may delay project setup, fund expenditures, or continuation of awards.

III. Research Security Training Requirements for NIH (NOT-OD-26-017)

In accordance with Section 10364 of the Chips and Science Act of 2022, NIH requires that all senior/key personnel listed on a NIH grant application must certify that they have completed Research Security Training (RST) within 12 months of the date of application submission on their CPOS. Completion of the RST will be effective for applications submitted for due dates on or after **May 25, 2026.**

PAVIR will accept either of the following modules to fulfill the NIH-required Research Security Training:

1. SECURE Center Condensed RST Module: https://www.secure-center.org/individual-training

Stanford Research Security Training (DOR-2000) in STARS (requires SUNet ID to access): https://ora.stanford.edu/resources/proposal-preparation-resources/research-security-training