VUMC Programs and Actions to Fulfill CHIPS & Science Act and NSPM-33 Research Security Program Requirements

The summary below highlights the research security programs and activities VUMC has established in alignment with NSPM-33. The January 2022 NSTC report titled "Guidance For Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development" was used to create the outline for this document. The July 2024 OSTP Memo titled "Guidelines for Research Security Programs at Covered Institutions" was also useful for preparing this outline.

Additionally, programs responsive to the CHIPS & Science Act are outlined later in the document.

VUMC RESEARCH SECURITY PROGRAM ELEMENTS (NSPM-33)

NSPM-33 requires a certification from research organizations awarded in excess of $50 million per year in total Federal research funding that they have implemented a research security program that includes the four elements highlighted in NSPM-33:

- Relevant VUMC Programs and Activities: NIH indicated in NOT-OD-25-161 that they are working with other federal agencies, to include NSF and DoD, to harmonize and finalize guidance on each of the required program elements and related certification processes. VUMC is prepared to comply with agency guidance once released.

(1) Cybersecurity

- Relevant VUMC Programs and Activities: See Appendix 1, "VUMC CYBERSECURITY PROGRAM ELEMENTS," following the document for a full program description

(2) Foreign travel security.

- Agencies should require that research organizations maintain international travel policies for faculty and staff traveling for organization business, teaching, conference attendance, research purposes, or any offers of sponsored travel that would put a person at risk.
    - Relevant VUMC Programs and Activities: VUMC's Finance Policy covering international travel requires that all employees 1) book travel through VUMC's contracted travel management company (World Travel) or the Concur booking platform; 2) submit an International Travel Questionnaire (ITQ) for review and approval by both VUMC Export Compliance (EC) and VUMC Enterprise Cybersecurity (VEC). Per the policy, approvals from both offices must be uploaded with the employee's expense report in order to be reimbursed.
- Such policies should include an organizational record of covered international travel by faculty and staff
    - Relevant VUMC Programs and Activities: VUMC: World Travel maintains records of international travel for all employees and shares that data with VUMC via 1) daily

report of international flight bookings sent to Global Support; 2) a direct data feed for all flights (international and domestic) into the travel tracker portal maintained by VUMC's contracted international emergency response company (International SOS (ISOS)), which is monitored by Global Support. ISOS also sends Global Support an international travel report with employee, dates of travel, destination (including destination risk ratings for health and security) on a weekly and quarterly basis.

and, as appropriate

- a disclosure and authorization requirement in advance of international travel,
  - Relevant VUMC Programs and Activities: See above finance policy requirements.
- security briefings,
  - Relevant VUMC Programs and Activities: Once an international flight is booked, ISOS automatically sends the traveler a pre-travel advisory email with health and security briefing information related to their destination. The advisory also encourages them to reach out to the Sr. Director of Global Support for higher risk destinations and encourages them to download the ISOS Assistance App for quick and easy access to real time health and security alerts, information, resources, etc. In addition to sending a pre-travel advisory at the time of booking, ISOS automatically sends real time alerts to the traveler that are specific to the traveler's destination and their dates of travel. The Sr. Director of Global Support also receives copies of these to ensure the team is aware of VUMC exposure and any support that travelers may require. Note that ISOS also has an employee portal with destination specific guidance and trainings (linked on the Global Support website) and they have a 24/7 emergency assistance phone number.
- assistance with electronic device security (smartphones, laptops, etc.),
  - Relevant VUMC Programs and Activities: See above finance policy requirements- VEC must review and approve.
- and preregistration requirements.
  - Relevant VUMC Programs and Activities: When travel is booked through Concur or World Travel, it is automatically registered in the VUMC/ISOS travel tracker portal. No action is required by the employee as this is automated. Travel to a country of concern also requires advanced pre-travel screening by the Global Support/Export Compliance and Office of Research teams.

(3) Research security training. Agencies should require that, as part of their research security programs, research organizations provide training to relevant personnel on research security threat awareness and identification, including insider threat training where applicable. Research organizations should consider incorporating relevant elements of research security into existing training on responsible and ethical conduct of research for faculty and students. In addition to periodic training, research organizations should conduct tailored training in the event of a research security incident.

- Relevant VUMC Programs and Activities: VUMC requires all principal investigators to take annual research security training, regardless of whether they plan to submit new grant applications. Other research staff must complete training if required by a federal agency or prime recipient institution (with whom we are contracting) or if serving as senior/key personnel on ANY sponsored project. The annual deadline is January 15. The training is offered through the CITI program, and meets all requirements outlined in the CHIPS & Science Act (risk mitigation, cybersecurity, international collaborations, foreign interference, transparency and disclosure requirements). We selected the CITI "Research Security: A Basic Course" to fulfill each of these requirements, plus additional NIH-specific disclosure information as required to meet NIH NOT-OD-25-133. Investigators may instead complete a different training module that meets all CHIPS requirements (e.g. NSF full or condensed modules) plus review the disclosure sections of the CITI module. See description of the tracking/certification plan in the "(Sec. 10634) Research Security Training" section under the CHIPS and Science Act header below.
- Investigators access training through: https://www.vumc.org/oor/research-security-training

(4) Export control training, as appropriate. Agencies should require that research organizations conducting R&D that is subject to export control restrictions provide training to relevant personnel on requirements and processes for reviewing foreign sponsors, collaborators and partnerships, and for ensuring compliance with Federal export control requirements and restricted entities lists.

- Relevant VUMC Programs and Activities: VUMC maintains an export control training module in two separate learning management platforms (FOTO & LMS) to ensure it is available to all faculty and staff. The modules were fully updated and rolled out in mid-2025 with all new auto-enrollment (based on defined criteria), reporting capabilities, and oversight management between the Export Compliance, Office of Faculty & Medical Staff Engagement, and Business Education teams.
- The EC module is available in LMS at https://learningexchange.vumc.org/. The *Export Compliance Education for VUMC* module is open enrollment, available to all staff/faculty, and takes 15-20 minutes to complete.

(5) Point of Contact. Agencies should require that, as part of their research security program, research organizations designate a research security point of contact (POC) and provide publicly accessible means to contact that individual (such as through a website or social media).

- Relevant VUMC Programs and Activities: VUMC has designated a Research Security POC: Susan Meyn, Associate Vice President for Research Resources and Senior Director of the Office of Research. Contact information is posted and publicly available on the Office of Research website here: https://www.vumc.org/oor/researchsecurity

ADDITIONAL VUMC PROGRAM ELEMENTS (CHIPS & SCIENCE ACT)

(Sec. 10634) Research Security Training. Each federal research agency shall establish a requirement that, as part of an application for a research and development award from the agency

- each covered individual listed on the application for a research and development award certify that each such individual has completed within one year of such application research security training that meets the guidelines developed under this section, and
- each institution of higher education or other organization applying for such an award certify that each covered individual who is employed by such institution or organization and listed on the application has completed such training.
    - Relevant VUMC Programs and Activities: See description of research security training annual requirement in "(3) Research security training" section above. Through CITI, the Office of Research maintains records of all VUMC employed faculty and staff who have completed research security training. The Office of Research and Office of Sponsored Programs update internal records at least monthly and/or upon request, so that the Office of Sponsored Programs may certify each key personnel's training completion status prior to submission of the funding application. VUMC is ready to comply with specific guidance from federal agencies.

(Sec. 10632) Prohibition on Malign Foreign Talent Recruitment Programs. Each federal research agency shall establish a policy that, as part of a proposal for a research and development award from the agency

- each covered individual listed in such proposal certify that each such individual is not a party to a malign foreign talent recruitment program in the proposal submission and annually afterwards for the duration of the award; and
- each institution of higher education or other organization applying for such an award certify that each covered individual who is employed by such institution of higher education or other organization has been made aware of the requirements under this section and complied with the requirement listed above.
    - Relevant VUMC Programs and Activities: VUMC expressly prohibits participation in a malign foreign talent program. The VUMC "Participation in Foreign Talent Recruitment Programs" policy is effective as of July 2024. The policy defines Foreign Talent Recruitment Programs and outlines acceptable and prohibited international collaboration activities. The policy is available at: https://powerdms.com/link/VanderbiltUMC/document/?id=2355548
    - Investigators fill out the VUMC international activity review (IAR) form (https://redcap.link/IAR) for any activity, whether formal or informal, that involves a

country of concern. This includes research collaborations, hosting visiting scholars or short-term foreign visitors, foreign grant/award opportunities, international travel, adjunct/adjoint faculty appointments, etc. The IAR submission is reviewed by the VUMC Office of Research (OOR) and VUMC Export Compliance (EC). Following initial review, OOR and EC may request additional review by the Office of Legal Affairs, Office of Faculty & Medical Staff Engagement, VUMC Immigration, VUMC Enterprise Cybersecurity, and/or other relevant partners.

- Activities deemed high risk due to compensation, involvement of listed entities, unusual contact methods, or any "Type 1" or "Type 2" activities as defined in the VUMC policy are prohibited. OOR and/or EC may meet with the investigator and, if needed, the department chair to discuss any concerns or possible mitigations. If needed, the case will be escalated to an Executive Committee comprised of 4-5 senior executive leaders for an official determination.
- Standard activities deemed low risk, such as those defined in the VUMC policy as acceptable "international collaboration activities," will be screened for appropriate mitigation factors. OOR and EC will work with the investigator and appropriate campus partners to ensure mitigations are in place before approving these activities.
- ALL international support, including all in-kind/non-monetary support, must be disclosed through the staff or faculty conflict of interest process as soon as possible. OOR reminds faculty to submit timely disclosures in follow-ups to IAR submissions. Additionally, each workforce member is required to submit a conflict of interest disclosure at least annually. The staff and faculty surveys contain detailed questions that are designed to capture any foreign support and any participation in a foreign talent recruitment program (whether or not malign).
- Contracts processed by the Office of Sponsored Programs - Contracts Management are screened by OOR if there is country of concern involvement. If there are any questions about entity ownership, the outside party will be asked to fill out the "entity questionnaire" with detailed questions about shareholders and their locations, including direct questions about country of concern shareholders.

APPENDIX 1: VUMC CYBERSECURITY PROTOCOLS & PROCEDURES

Agencies should require that research organizations satisfy the cybersecurity element of the research security program requirement by applying the following basic safeguarding protocols and procedures:

- Provide regular cybersecurity awareness training for authorized users of information systems, including in recognizing and responding to social engineering threats and cyber breaches.
    - Relevant VUMC Programs and Activities:
        - VUMC has a comprehensive training program related to cybersecurity.
            - All employees complete standard compliance training at the time of hire and then annually. This compliance training includes sections on cybersecurity, HIPAA, and privacy.
            - By policy, HIPAA training is required prior to receiving access to Individually Identified Health Information.
            - VUMC conducts regular phishing awareness campaigns.
            - The VUMC Business Information Security team performs Cybersecurity outreach across the VUMC enterprise.
            - The VUMC Cybersecurity website provides updated training materials, policies and SOPs, and contact information for the benefit of all VUMC staff.
            - VUMC Cybersecurity staff are provided with professional development opportunities, such as cybersecurity training and conferences, annually.

- Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
    - Relevant VUMC Programs and Activities:
        - Authentication, authorization, and access to electronic systems are governed by the following policies and procedures:
            - *Authentication to Electronic Systems and Applications*
            - *Authorization and Access to Electronic Systems and Applications*
            - *Electronic Identity / VUMC ID Management (SOP)*
            - *Password Management (SOP)*
            - *VUMC Approved Authentication (SOP)*
        - Authorized users are managed via an enterprise directory and use single sign on (SSO) to authenticate to enterprise applications and systems. Per policy, systems containing sensitive data require the use of multi-factor authentication (MFA).

        - Applications and systems that do not support SSO are required to have a documented exception, which outlines compensating controls used in place of SSO.
        - Applications and systems that do not support MFA are required to have a documented exception, which outlines the compensating controls used in place of MFA.
    - VUMC verifies the identity of all individuals accessing VUMC systems. By policy, this verification requires a form of government issued identification.

- Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
    - Relevant VUMC Programs and Activities:
        - Authorization is governed by the *Authorization and Access to Electronic Systems and Applications* policy.
        - Authorized users are managed via an enterprise directory and use single sign on (SSO) to authenticate to enterprise applications and systems. Per policy, systems containing sensitive data require the use of multi-factor authentication (MFA).
            - Applications and systems that do not support SSO are required to have a documented exception, which outlines compensating controls used in place of SSO.
            - Applications and systems that do not support MFA are required to have a documented exception, which outlines the compensating controls used in place of MFA.

- Verify and control/limit connections to and use of external information systems.
    - Relevant VUMC Programs and Activities:
        - Access to external information systems is governed by the following policies and procedures:
            - *Internet Monitoring and Filtering*
            - *Application Inventory (SOP)*
        - VUMC has a comprehensive and continuously improving zero-trust program.
        - Traffic to external information systems is monitored using a complementary set of tools at both the network and endpoint levels.
        - VUMC blocks access from internal networks to external resources and applications that pose unnecessary risk to VUMC.

- Control any non-public information posted or processed on publicly accessible information systems.
    - Relevant VUMC Programs and Activities:

- By policy, non-public information is not posted to or processed on publicly accessible information systems.
- VUMC performs legal, technical, and cybersecurity reviews of external entities prior to sharing data.
- VUMC employs sensitivity labels on electronic communications to help mitigate the risk of inadvertent exposure of non-public data.
- By policy, non-public data is encrypted at-rest and in-transit.

- Identify information system users, processes acting on behalf of users, or devices.
  - Relevant VUMC Programs and Activities:
    - Authentication, authorization, and access to electronic systems are governed by the following policies and procedures:
      - Authentication to Electronic Systems and Applications
      - Authorization and Access to Electronic Systems and Applications
      - Electronic Identity / VUMC ID Management (SOP)
      - Password Management (SOP)
      - VUMC Approved Authentication (SOP)
    - Authorized users are managed via an enterprise directory and use single sign on (SSO) to authenticate to enterprise applications and systems. Per policy, systems containing sensitive data require the use of multi-factor authentication (MFA).
      - Applications and systems that do not support SSO are required to have a documented exception, which outlines compensating controls used in place of SSO.
      - Applications and systems that do not support MFA are required to have a documented exception, which outlines the compensating controls used in place of MFA.
    - VUMC verifies the identity of all individuals accessing VUMC systems. By policy, this verification requires a form of government issued identification.

- Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
  - Relevant VUMC Programs and Activities:
    - Authentication, authorization, and access to electronic systems are governed by the following policies and procedures:
      - Authentication to Electronic Systems and Applications
      - Authorization and Access to Electronic Systems and Applications
      - Electronic Identity / VUMC ID Management (SOP)
      - Password Management (SOP)
      - VUMC Approved Authentication (SOP)

        - Authorized users are managed via an enterprise directory and use single sign on (SSO) to authenticate to enterprise applications and systems. Per policy, systems containing sensitive data require the use of multi-factor authentication (MFA).
            - Applications and systems that do not support SSO are required to have a documented exception, which outlines compensating controls used in place of SSO.
            - Applications and systems that do not support MFA are required to have a documented exception, which outlines the compensating controls used in place of MFA.
        - VUMC verifies the identity of all individuals accessing VUMC systems. By policy, this verification requires a form of government issued identification.

- Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
    - Relevant VUMC Programs and Activities:
        - VUMC has a comprehensive and continuously improving zero-trust program.
        - Traffic to external information systems is monitored using a complementary set of tools at both the network and endpoint levels.
        - VUMC blocks access from internal networks to external resources and applications that pose unnecessary risk to VUMC.
        - VUMC employs sensitivity labels on electronic communications.
        - VUMC utilizes data loss prevention tools natively within its productivity suite and through packet inspection at the network level.

- Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
    - Relevant VUMC Programs and Activities:
        - VUMC employes industry best practices to isolate internal resources from public access. By policy and practice, VPN and MFA are required for external access to internal VUMC resources.

- Provide protection of scientific data from ransomware and other data integrity attack mechanisms.
    - Relevant VUMC Programs and Activities:
        - VUMC data is backed up in compliance with VUMC operational, regulatory, and business agreement requirements. Backup and retention methodologies incorporate appropriate physical and technical safeguards to ensure Information System confidentiality, integrity, and availability

(recoverability). In addition, backups are tested and verified on a regular basis.

- Identify, report, and correct information and information system flaws in a timely manner.
    - Relevant VUMC Programs and Activities:
        - VUMC performs regular scanning of assets. This scanning includes the identification of out-of-date, malicious, or otherwise unwanted applications and systems.
        - By policy, systems flaws and vulnerabilities must be patched according to stated timelines based on the nature of the vulnerabilities and the risk profile of the system.
        - An incident response plan is in place in order to appropriately identify and respond to both internal and external threats.

- Provide protection from malicious code at appropriate locations within organizational information systems.
    - Relevant VUMC Programs and Activities:
        - VUMC has a comprehensive and continuously improving zero-trust program.
        - A complementary set of endpoint management and protection tools are deployed on resources across the enterprise. These tools are updated on a regular basis and perform both file based and heuristic analysis of endpoint and network activity.

- Update malicious code protection mechanisms when new releases are available.
    - Relevant VUMC Programs and Activities:
        - VUMC has a comprehensive and continuously improving zero-trust program.
        - A complementary set of endpoint management and protection tools are deployed on resources across the enterprise. These tools are updated on a regular basis and perform both file based and heuristic analysis of endpoint and network activity.

- Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.
    - Relevant VUMC Programs and Activities:
        - VUMC has a comprehensive and continuously improving zero-trust program.
        - A complementary set of endpoint management and protection tools are deployed on resources across the enterprise. These tools are updated on a regular basis and perform both file based and heuristic analysis of endpoint and network activity.

- Additional cybersecurity requirements, for example, those provided by the National Institute of Standards and Technology (NIST), will apply in some cases, such as for research involving classified information or CUI.
    - Relevant VUMC Programs and Activities:
        - VUMC has an Information Security Compliance Review policy and procedure for assessing systems containing CUI.
        - Systems are assessed per project; thus, an assessment will need to be performed to determine which standards are applicable for the system and associated data classification. VUMC can then attest that the system meets the applicable standards and/or has compensating controls in place.
        - Additionally, VUMC has established a Research Compliance Committee and Research Security Workgroup to ensure that the organization stays informed of all newly enacted research regulations and rules to determine where they may apply to VUMC's assessment procedures.