Maintaining the Security and Integrity of America’s Research Enterprise

March, 2021

The White House Office of Science and Technology Policy

www.whitehouse.gov/ostp
www.ostp.gov
@WHOSTP

Key takeaways

- The integrity of the research enterprise rests upon core principles and values.
- Principled international collaboration and foreign contributions are critical to the success of the U.S. research enterprise.
- Some individuals and foreign governments violate core principles of integrity and pose risks to research security.
- Hidden diversions of intellectual property weaken the U.S. innovation base and threaten our security and economic competitiveness.
- ***The U.S. Government is taking deliberate steps to address risks to research security and integrity while maintaining an open and collaborative enterprise.***
- ***Research organizations should adopt policies and practices that will help preserve openness and collaboration while maintaining the security and integrity of the research enterprise.***

U.S. GOVERNMENT ACTION TO MAINTAIN RESEARCH SECURITY AND INTEGRITY

Coordinated U.S. government action will help preserve openness and collaboration while maintaining the security and integrity of the research enterprise

National Security Presidential Memorandum 33 (NSPM-33) established national security policy for U.S. government-supported R&D:

- Provides direction for Federal departments and agencies
- Establishes roles and responsibilities related to research security and integrity
- Outlines specific actions the Federal government will take to enhance research security and integrity
  - Enhance awareness of research security risks and protections
  - Strengthen disclosure requirements and processes
  - Limit/Manage access and participation
  - Vetting foreign students and researchers
  - Information sharing
  - Research security training
  - Risk identification and analysis
  - Promote and protect international R&D cooperation

Enhance awareness of research security risks and protections

- ***OSTP and other agencies will engage with the R&D enterprise to enhance awareness of risks to research security and integrity, and policies and measures for mitigating these risks***:
  - Explain threats, Federal policies, and actions to mitigate risks
  - Promulgate guidelines for research organizations
  - Increase awareness about existing law, regulations, and other protection mechanisms
- ***ODNI will coordinate with relevant agencies to develop information products related to research security that are suitable for sharing with government and non-government entities***:
  - Explain collection methods and means of exploitation
  - Help identify R&D activities and collaborations with significant risk of exploitation
  - Provide counterintelligence awareness training

Strengthen disclosure requirements and processes

- ***Funding agencies will require disclosure of information related to potential conflicts of interest and commitment***
  - Specific requirements depend on individual's role in the research enterprise
  - Disclosures provided to the organization, funding agency, or both, consistent with funding agency policies.
  - Agencies will ensure that individuals have reasonable recourse to correct or address inaccurate or incomplete information.
- ***Agencies will standardize disclosure policies, processes, definitions, and forms to the extent practicable***
  - Agencies will integrate digital persistent identifiers (DPIs) into disclosure processes where appropriate and practicable.
- ***Identifying and investigating noncompliance***
  - Agencies will work with relevant entities to strengthen mechanisms and capabilities to identify and investigate potential violations of disclosure requirements.
- ***Agencies will ensure appropriate and effective consequences for violation of disclosure requirements***
  - May consider a range of consequences depending on the nature of the violation

Limit/manage access and participation

- ***Agencies will ensure policies and processes to control and track access to and utilization of U.S. Government research facilities, to include:***
  - Controlling and tracking physical access
  - Vetting and securely hosting foreign visitors
  - Evaluating research partnerships or contracts with outside entities
- ***Agencies will prohibit their Federal personnel who are also participants in the U.S. R&D enterprise from participating in foreign government-sponsored talent recruitment programs.***
  - Agency-specific policies may extend prohibition to contractor personnel
  - Agencies may provide exemptions where appropriate

Vetting foreign students and researchers

- ***DOS and DHS* will to ensure that vetting processes reflect the changing nature of the risks to U.S. R&D**
  - Apply a risk-based process to vet visa applicants
  - Ensure that consular officers may collect and consider relevant information related to research security and integrity

Information sharing

- To help strengthen the effectiveness of response measure:
- ***Agencies will share information about individuals who violate research security policies with Federal funding and other relevant agencies, where consistent with privacy laws and other legal restrictions.***

Research security training

- ***Federal agency personnel conducting R&D activities or participating in the process of allocating Federal R&D funding will receive annual research security training.***
  - Risks to the U.S. R&D enterprise
  - Individuals' responsibilities related to research security and integrity
  - Circumstances and behaviors that may indicate risk to research security and integrity

Risk identification and analysis

- ***Funding agencies will require that research organizations receiving Federal science and engineering support in excess of $50 million per year certify that they have established and operate a research security program.***
- Programs should include the following elements:
  - Cyber security
  - Foreign travel security
  - Insider threat awareness and identification
  - Export control training (as appropriate)
- ***Funding agencies will consider whether additional program requirements are appropriate for organizations receiving funding in critical and emerging technology areas.***

Promote and protect international R&D cooperation

- ***DOS will coordinate with other agencies to engage with foreign allies and partners to promoting policies and practices that increase awareness of risks to research security and improve cooperation on international protection and response efforts.***
- Messaging will be designed to increase awareness and encourage foreign governments to undertake effective practices to assess and mitigate risks to research security and integrity.

RECOMMENDED PRACTICES FOR RESEARCH ORGANIZATIONS TO MAINTAIN RESEARCH SECURITY AND INTEGRITY

Research organizations can adopt policies and practices that will help preserve openness and collaboration while maintaining the security and integrity of the research enterprise

- Universities and other research organizations play a critical role in the security and integrity of America's research enterprise, complementing the role of the Federal Government.
- Research organization policies designed to protect research integrity in many cases also help guard against behaviors that pose national security risk.
- Recommended practices for enhancing research and security and integrity span five broad categories:

  I. Demonstrate organizational leadership and oversight

  II. Establish an expectation of openness and transparency

  III. Provide and share training, support, and information

  IV. Ensure effective mechanisms for compliance with organizational policies

  V. Manage potential risks associated with collaborations and data

- Implementation of policies and practices should evolve thoughtfully and appropriately to meet current and future challenges, including foreign government efforts to exploit or interfere with the research enterprise.

Recommendations to demonstrate organizational leadership and oversight

- ***1. Convey the importance of research security and integrity at the leadership level***
  - Leaders should consistently and regularly message the importance of research security, along with actions they are taking to ensure that security is balanced with openness.
- ***2. Ensure an organizational approach to research security***
  - Develop written research security implementation plans
  - Designate a chief research security officer or equivalent to oversee research security management
- ***3. Establish cross-organizational working groups and task forces to discuss, develop, implement, and evaluate research security strategies***
- ***4. Establish and operate a comprehensive research security program***
  - Develop a "risk profile" that assesses potential risks associated with loss of research data and IP and the potential for significant commercial or national security impacts
  - Should include elements of cyber security, foreign travel security, insider threat awareness and education, and export control training. (Will be required for organizations receiving at least $50M in annual Federal R&D funding)
  - Economies of scale may be realized by coordinating with other organizations.

Recommendations to establish an expectation of openness & transparency

- **5. *Establish and administer policies and practices regarding COI/COC and disclosure***
  - Assist employees, affiliates, and students with compliance with funding agency disclosure requirements. Administrative burden may be minimized by using online forms that allow updates while maintaining a record of prior disclosures.
  - Encourage or direct researchers to consult a designated organizational official when in doubt about any matter regarding research security or integrity, include any prospective participation in foreign government-sponsored talent recruitment programs, which often provide contracts directly to researchers with the expectation of their signature alone.
- **6. *Require disclosure of information necessary to identity and assess potential COI/COC***
  - Require for employees/affiliates engaged in the research enterprise, regardless of whether involved in Federally-funded projects, including researchers, graduate students engaged in research, and long-term visiting scholars
  - Recommended disclosure content parallels requirements for Federally-supported R&D
- ***7. Ensure compliance with DOS and DHS requirements for reporting foreign student & researcher information***
- ***8. Establish policies regarding digital persistent identifiers (DPIs)***
  - Many potential benefits, including streamlining grant application processes via pre-population of forms
  - Establish policies regarding requirements for research enterprise employees, contractors, and affiliates to be registered with a service that provides a DPI, and to provide access to relevant information disclosed through the DPI (e.g., employment, research funding, professional R&D affiliations, published research)
- **9. *Ensure compliance with Section 117 requirements for reporting foreign gifts and contracts***

Recommendations to provide and share training, support, and info

- ***10. Provide training to participants in the research enterprise on the responsible conduct of research***
  - Offer to all researchers, irrespective of funding source
  - Content should include disclosure requirements and processes, upholding core organizational values, and IP protection
- ***11. Provide guidance for those considering participation in foreign government-sponsored talent recruitment programs.*** To the extent feasible, assist in reviewing contracts and understanding implications of commitments and any potential for exploitation.
- **12. *Partner with local FBI field offices to strengthen research security.*** FBI can help with insider threat and cybersecurity programs; awareness training to help recognize suspicious behavior and better protect personnel, facilities, info.
- **13. *Ensure awareness of circumstances and behaviors that may pose a risk to research security and integrity***
  - Potential risk factors in conditions, contract terms, or other obligations associated with participation in/with foreign government-sponsored programs and entities (Examples provided)
  - Obligation to conduct R&D on behalf of another entity without knowledge and approval of the employing organization
  - Association with foreign entities identified on the U.S. government's Consolidated Screening List
- **14. *Share information regarding potential violations of disclosure policies***
  - Share with relevant funding agencies; ensure compliance with any such requirements regarding
  - Work with funding and law enforcement agencies to determine appropriate conditions and mechanisms for the provision of such information

Recommendations to ensure effective measures for compliance with organizational policies

- ***15. Establish and exercise effective means of discovering activities that threaten research security and integrity***
  - Develop means to identify potentially problematic relationships and instances where disclosures are incomplete or inaccurate
- ***16. Ensure appropriate and effective consequence for violation of disclosure requirements***
  - Depending on the nature of the violation, consider a range of potential consequences (e.g., grant termination or personnel replacement, probation, revocation of tenure)
- **17. *Include in employment agreements provisions that support research security and integrity.*** Consider provisions that:
  - Establish clear expectations regarding activities outside the employment agreement period (e.g., summer months)
  - Establish clear expectations regarding research security training and adherence to codes of conduct
  - Allow organizations to take effective actions against individuals who violate policies

Recommendations to manage potential risks associated with collaborations and data

- **18.** ***Establish a centralized review and approval process for evaluating formal research partnerships***
  - Establish a process to assess risk to the security or integrity of the research enterprise, and to protect individual and organizational interests. Recommended evaluation factors include affiliations of outside entities, IP value, and export control considerations.
- **19.** ***Establish and operate a risk-based security process for foreign travel review and guidance***
  - Could include programs for reviewing travel for export compliance, software use restrictions, and other safety and security concerns. Potential program elements include required notifications, device security measures, and security briefings.
- **20.** ***Manage potential risks associated with foreign visitors and visiting scholars***
  - Establish requirements for vetting and securely hosting foreign visitors to mitigate potential risks (e.g., required notifications, research security/integrity training for visitors, screening for restricted/denied parties)
- **21.** ***Establish and maintain effective data security measures***
  - Work continually to identify and implement measures to improve data security, internal breach prevention, and incident response processes
  - Consider elements of the NIST Cybersecurity Framework

Conclusion

- Implementing these government actions and recommendations for research organizations will help protect the security and integrity of the American and international R&D enterprises, while preserving the open and collaborative nature that has been critical to U.S. leadership in R&D.
- This will help ensure that scientists and students—both U.S. and foreign national—who follow laws, regulations, policies, and codes of conduct will be welcome and supported within a vibrant and secure enterprise that remains a desirable destination for researchers across the world.
- Success in this endeavor will require partnership and cooperation across the R&D enterprise, including the Federal Government, research organizations, private companies, and non-government organizations.
- Together, we can uphold the principles that bolster the integrity of our research enterprise, strike the right balance between openness and security, and ensure that the United States continues to engage in productive collaboration and remains a global leader in S&T