NIST IR 8484 – Review Checklist for Research Security Plans

	Y	N
1. Has the awardee provided a research security point of contact with contact information?*		
2. Does the research security plan include establishing a research security team?*		
3. Does the research security team reflect broad expertise (e.g., research, export controls, cybersecurity)?		
4. Does the research security plan include establishing methodologies and processes to assess and mitigate risks to at-risk technology and IP throughout the project?		
5. Does the research security plan include establishing processes to review personnel appointments and to address conflicts of interest or conflicts of commitment, including malign foreign affiliations?*		
6. Does the research security plan include establishing a training program that meets NSPM-33 requirements (e.g., foreign travel, research security, export control)?*		
a. Does it describe the scope and frequency of the required training?		
7. Does the research security plan include review, approval, and reporting of collaboration and publication requests?		
8. Does the research security plan include technology control plans for cybersecurity and export controls?*		
a. Does it describe measures to restrict access to data and systems by unauthorized personnel?		
b. Does it describe the incident response plan?		
c. Does it describe measures to ensure compliance with federal export regulations?		
9. Does the cybersecurity program described maintain consistency with NSPM-33 (e.g., NIST Cybersecurity Framework 2.0, 800-171)?		
10. Does the research security plan include an implementation timeline that clearly identifies dates that all aspects of the plan will become operational?*		

For Reference: Overview of Research Security Plan Requirements per NSPM-33

- **Cybersecurity** – The applicable NOFO describes the cybersecurity requirements for the Research Security Plan, based on program and the risks of foreign exfiltration of research data and resulting technology. The Plan should integrate information technology (IT) security system elements, including cybersecurity, to establish a risk-balanced approach to determine logical access to science and research information resources, as well as how and when that access is managed.[1]
- **Foreign travel security** – Requires periodic training (at least once every six years) on foreign travel security for covered individuals, "engaged in international travel, including sponsored international travel, for organization business, teaching, conference attendance, or research purposes." Also requires covered institutions to implement a travel reporting program "for covered individuals participating in R&D awards when a federal research agency has determined that security risks warrant travel reporting in accordance with the terms of an R&D award."
- **Research security training** – Institutions are required to implement a research security training program, "for all covered individuals to address the unique needs, challenges, and risk profiles of covered individuals and to certify that the institution ensures that each such covered individual completes such training." There is some flexibility given to institutions here, as it allows them to use NSF's training modules or certify that covered researchers have completed a program with similar components.
- **Export control training** – Requires covered institutions to certify that they require "covered individuals who perform R&D involving export-controlled technologies, to complete training on U.S. export control and compliance requirements." Again, some flexibility is provided here, allowing institutions to use the training offered by the Bureau of Industry and Security of the Department of Commerce, Directorate of Defense Trade Controls at the Department of State, or a training program with similar components.

[1] In the future (within one year after NIST finalizes a resource for research institutions), institutions of higher education will be required to institute a cybersecurity program consistent with the NIST publication. Non-institutions of higher education will be required to certify implementation of applicable cybersecurity requirements.