NIST IR 8484 Research Security General Operations Checklist (8484 GOC)

Performing research security reviews of grant proposals is critical to protecting the U.S. supply chain and the research ecosystem of emerging semiconductor and microelectronic technologies that are essential to U.S. economic and national security.

Research Security Reviews consider a myriad of key questions that apply to covered institutions and covered individuals. Answers to key questions are obtained through open-source intelligence (OSINT) as well as information provided by the funding opportunity applicant. Table 1 is a NIST IR 8484-derived general operations checklist (8484 GOC). This is a consolidated list (non-inclusive) of the key questions extending across the five review categories (researchers, travel, products & services, funding opportunities, and publications & collaborations) and the five checklists included in NIST IR 8484 Appendix D. The use of 8484 GOC addresses the research-security criteria contained within federal initiatives (NSPM-33, CHIPS & Science Act, SBIR/STTR Due Diligence Act).

Table 1. NIST IR 8484 Research Security Framework General Operations Checklist (8484 GOC) is a non-inclusive list of key research security questions for reviewing researchers, foreign travel, products & services, funding opportunities, and publications & collaborations.

NIST IR 8484 Research Security Framework General Operations Checklist (8484 GOC)		
Institution	**Individual**	**Both**
FOCI – Foreign Ownership Control and Influence	Conflicts of Interest	ITA Consolidated Screening / Entity List
Foreign Obligations	Conflicts of Commitment	Capabilities match request
Cybersecurity	Foreign Education	Military / Civil applications
Data management	Foreign Talent Recruitment Programs (Benign and Malign)	
Export Control and Compliance	Malign foreign affiliations (e.g., Universities, Confucius Institutes, Organizations, Professional Memberships, Scholarships, Awards, etc.)	
Venture Capital	Position sensitivity - Access (CUI / Intellectual Property / Technology)	
Research Security Plan / Program	Foreign publications/Patents	
	Scholarships / Awards	
	Professional Associations	
	Foreign travel (e.g., conferences, symposiums, and meetings)	

A Research Security Review is a collaborative decision-making process between the Team and organizational management consisting of a risk/benefit recommendation by the Team to organizational management for a final risk determination. The composite analysis of the information acquired and assessed during a research security review results in a risk-balanced determination of low, medium, or high risk contained within the Research Security Review Form. A no risk determination is impractical as achieving a no risk security posture is unrealistic and can be deceptive of underlying risk to customers, asset owners, and research security practitioners. A low-risk determination concludes that the risk is acceptable and that the benefits to the organization clearly outweigh the risk. A medium risk determination concludes that an identified risk exists, and that the risk can be mitigated through the deployment of available security countermeasures to achieve an acceptable risk/benefit determination. A high-risk determination concludes that a targeted collection risk exists, and that the deployment of available security countermeasures may be insufficient to achieve an acceptable risk/benefit determination resulting in a rejection of the grant application. Targeted high-risk collection threats may require validation from non-OSINT sources.