



Women Advance: Research Security

Fellowship to Advance the Leadership of Women in Research Security

Competition Opens:	May 3, 2024
Application Deadline:	May 24, 2024
Eligibility:	<ul style="list-style-type: none"> • Argentinian and South African women nationals. • Mid-career or senior administrators, compliance managers, department heads, or research directors at science and technology research institutions. • Demonstrates existing knowledge and understanding of research security and integrity concepts. • Ability and willingness to commit to all phases of the program outline. • Proficiency in the English language.
How to Apply:	<p>Please submit the required documents in the online application portal: https://insights.crdfglobal.org/womenadvance2024app</p> <p>For additional questions regarding the fellowship please contact: womenadvance@crdfglobal.org</p>
Required Documents:	<ol style="list-style-type: none"> 1. The completed application, which should be submitted in the application portal 2. National ID/passport 3. CV 4. Institutional letter of support
Fellowship Duration:	Up to five (5) months

Overview

CRDF Global, on behalf of the U.S. Department of State, is pleased to announce the launch of **Women Advance: Research Security**. This remote fellowship will promote the leadership of women in research security to bolster nonproliferation by enhancing selected fellows’ research security knowledge, skills, and professional networks, as well as establish or solidify the selected candidates as research security leaders. This fellowship will include access to online training courses, provide discussion sessions with leading experts and counterparts, and pair fellows with experienced mentors. The fellowship will also include support for professional development opportunities, including travel to relevant conferences or meetings. Over this fellowship, selected



mentors will work with fellows to create and pursue individual development plans that will establish or further solidify them as research security leaders.

The fellowship is open to Argentinian and South African women nationals including mid-career or senior administrators, compliance managers, department heads, or research directors at a science and technology research institution. The candidates should be able to demonstrate existing knowledge and understanding of research security concepts. Applicants are required to submit an official institutional letter of support, on official letterhead, signed and dated by their supervisor confirming their approval of the applicant's participation in the program. The letter of support should clearly state applicant's full name, applicant's position title, institution name, and supervisor's consent to fellowship duration.

The professional development support included in the fellowship will include up to \$3,000 per fellow. This may be used to support travel to relevant conferences, trainings, or meetings as well as activities to enable the fellows to implement or enhance research security policies, practices, and procedures within their institutions, sectors, and the wider region to secure sensitive research, knowledge, technology, while taking initial steps to build a multi-national consortium of women leaders in this field.

Fellowship Scope

This fellowship will support leading women in research security by:

- Increasing their knowledge, skills, and abilities as research security leaders within their sector, country, and region to effectively manage and mitigate risks associated with the field through trainings, access to the latest tools and technologies, and deeper understanding of international best practices and standards in research security;
- Establishing connections between the fellows and prominent leaders in the field to create a robust support and advocacy network, which will persist into the future. This network will not only foster collaboration and mentorship but will also include the active participation of inspiring women leaders, emphasizing diversity and empowerment in leadership roles;
- Enhancing their comprehension of foreign risks to research, expand their knowledge on the practical implementation of research security policies and practices both regionally and globally and deepen their understanding of the challenges and considerations that institutions encounter when implementing these measures;
- Building their leadership skills to be influential players in their field and advancing their careers by furthering credentials as leaders within their institutions and country;
- Ensuring the fellows possess knowledge and skills to help develop detailed documents that outline standardized procedures and best practices for handling sensitive data, using secure communication channels, and protecting intellectual property at research institutions, and
- Providing the fellows with tools and competencies to help in planning mitigation strategies and ensuring compliance with regulatory requirements as well as conduct comprehensive trainings and design training modules focused on topics such as data protection, cybersecurity measures, ethical considerations, intellectual property protection, common challenges faced when developing and implementing research security compliance policies, foreign threats to research, talent, and intellectual property



in different regions, and building networks among women working in research security for researchers and staff.

Program Outline:

- 1. Online training course:** Selected fellows will participate in an asynchronous course consisting of at least nine pre-recorded modules. The virtual training series will help selected fellows to enhance their comprehension of research security risks, expand their knowledge on the practical implementation of research security policies and practices both regionally and globally, and deepen their understanding of the challenges and considerations that institutions encounter when implementing these measures. Fellows will learn to secure research, talent, and intellectual property, understand the dual-use potential of select types of intellectual property, protect data while catalyzing research collaboration, conduct research security risk assessments, identify common challenges faced when developing and implementing research security compliance policies, and gain buy-in and build coalitions to enact sustained change at academic institutions.
- 2. Live expert sessions:** Selected fellows will have an opportunity to meet with women security leaders (e.g. leaders of U.S., international, and regional research institutions, former and current leaders of governmental and non-governmental organizations focused on research security and compliance, and senior experts on research security, among others) in at least six live remote sessions. The fellows can expect to be actively involved in conversations regarding challenges developing and implementing research security compliance policies, building networks among women working in research security, identifying research security gaps, and closing gaps in research security practices.
- 3. Mentorship:** Selected fellows will be matched with experts to meet virtually at a frequency to be determined between the mentors and mentees (at least once monthly). The mentors will assist the mentee with professional development support. Mentors will work with fellows to design, develop, and make progress on an individual development plan designed to enhance their ability to advance research security, meet fellows' specific development goals, further establish fellows as research security leaders in their region.
- 4. Professional Development Support:** The activities included in the professional development support will enable the fellows to implement or enhance research security policies, practices, and procedures within their institutions, sectors, and the wider region to secure sensitive research, knowledge, technology, and talent from malign acquisition. The professional development activities will also contribute to the development of support and advocacy network for the fellows going forward. The activities will be identified by fellows, in close consultation with mentors, and can include professional memberships, trainings, speaking at conferences abroad, and travel support (total professional development support costs up to \$3,000 USD).
- 5. Individual Development Plan:** To navigate the mentorship and professional development support, each fellow will create an individual development plan. These plans will enhance procedures for identifying and mitigating research security threats, advance research security measures and talent protection strategies within the fellows' institutions, strengthen current protocols, training programs, and security systems to address evolving threats and vulnerabilities.



Eligibility

- Applicants must apply individually.
- Applicants must be Argentinian or South African women nationals.
- Applicants must be mid-career or senior research administrators, compliance managers, department heads, or research directors at a science and technology research institution in Argentina and South Africa.
- Applicants should have career objectives that align with goals of the project and can demonstrate existing knowledge and understanding of research security concepts.
- Applicants must be willing and able to commit to all phases of the program outline (approximately July–November 2024).
- Applicant must possess proficiency in the English language and all application materials must be submitted in English. Applicants receiving provisional notice of selection may be asked to provide additional information to determine eligibility.
- Applicants must submit an institutional letter of support to be considered for this fellowship.

Evaluation Criteria	
Relevance and Impact to the Fellowship Scope	<ul style="list-style-type: none">• The proposed fellowship must meet the expected scope and objectives, both short-term and long-term.• The application addresses the relevance of the fellowship to the applicant’s country and the wider research security industry.
Clarity, Completeness, and Detail of the Application	<ul style="list-style-type: none">• Every part of the application is completed, and all supporting documentation is submitted.
Past Performance	<ul style="list-style-type: none">• The applicant shows a track record of high-quality outcomes on matters relating to responsible science and research security.
Sustainability Potential and Commitment	<ul style="list-style-type: none">• Proven ability to continue to advance research security and integrity within the fellows’ institution and beyond following the end of the fellowship (e.g., in the region, in the research field at large, etc.)

Applicants receiving provisional notice of selection may be asked to provide additional information to determine eligibility for receipt of funds. For detailed information regarding general CRDF Global grant policies please visit: <https://www.crdfglobal.org/funding-opportunities/#information-applicants>.