**A red letter on a black background

Description automatically generated**

**Indiana University**

Chief Research Security Officer (CRSO) & Facility Security Officer (FSO)

Position Description

**Position Title**

Chief Research Security Officer (CRSO) & Facility Security Officer (FSO)

**Department**

RESEARCH SECURITY OFFICE (UA-RSO-IUBLA)

**Special Instructions Summary**

While a cover letter is not required, it is encouraged for a position at this level.  Otherwise, a cover letter will be requested at the onset of an interview.

**Job Summary**

The IU Research Security Office (RSO) was created by the Office of the Vice President for Research to address the security risks posed to the research environment at Indiana University and to assist researchers with efforts to protect themselves, their research data and methodologies, publication rights, and intellectual property.

Department-Specific Responsibilities

* Directs the Office for Research Security within IU Research.
* Oversees coordination with several IU divisions including IU Research, IU General Counsel, and International Affairs.
* Works with university leaders responsible for public safety and compliance, as well as state and federal oversight agencies to ensure the security of IU research, intellectual property, and associated systems.
* Serves as an advisor to the president of the university on issues related to research security and foreign influence.
* In addition, an active facility security clearance (FCL) authorized for the university by the Defense Counterintelligence and Security Agency (DCSA), a division of the U.S. Department of Defense, allows IU faculty to engage in classified research. As required by DCSA, the role of facility security officer (FSO) ensures the safeguarding of classified information and compliance of federal regulations under 32CFR117. To that end, this position involves coordinating the requirements for maintaining the FCL and ensuring the requisite infrastructure for IU faculty to engage in classified research.
* Responsible for coordination of the university's obligations related to research security. This includes ensuring coordination with compliance offices of the university (Export Control, Compliance Office and COIC, General Counsel's Office) for the assessment of and response to national security threats and other threats to research information and the research infrastructure.
* Responsible for the development and implementation of policies and other resources concerning research security, insider threat programs, and security of restricted and/or federally controlled data and information.
* Provides leadership in the execution of the research security vision and mission for IU Research for the entire university.
* Responsible for designing, developing, and implementing full research security strategic plans and exercises a high degree of autonomy and authority to interpret and set policies and priorities for all IU Research security initiatives.
* Must be able to provide recommendations to high levels of IU Research and University officials on a wide variety of complex security issues. Must be able to initiate and interface with USG officials in a variety of government and military agencies. The role requires independent decision-making authority, as well as the ability to collaborate closely with others, and will be responsible for recommending and implementing specific actions.
* Manage and initiate personnel clearances and process visit access requests (VARs) within the Defense Information Security System.
* Develops and manages prime and subcontract DD-254's.
* Serves as a main participant in DCSA Security Vulnerability Assessments (SVA) and Continuous Monitoring (CM) engagements. Conduct periodic self-inspections in accordance with 32CFR117 and research security policies as required by DCSA.
* Investigates, reports to DCSA industrial security representative (ISR), and documents security infractions and violations.
* Assists the ISSM to achieve NIST and CMMC 2.0 compliance.

General Responsibilities

* Participates on senior leadership teams to formulate strategic planning and the highest-level operational objectives for project management areas.
* Establishes long-term business plans and long-term strategic objectives.
* Manages projects to ensure on-time completion according to specifications and within budgeted costs.
* Directs leadership staff who provide supervision to program management teams.
* Responsible for escalated operational issues, including human resources and/or people management situations.
* Drives innovation and excellence to ensure program growth and success, reviews and creates policies and procedures.
* Determines overall budget for program management teams; reviews and approves financial proposals from direct reporting leaders; has significant fiscal responsibilities that require frequent interaction with executive leaders.
* Provides expertise and identifies grant and/or funding opportunities; develops business relationships across the university and externally.

**Qualifications**

*Combinations of related education and experience may be considered. Education beyond the minimum required may be substituted for work experience. Work experience beyond the minimum required may be substituted for education.*

EDUCATION

**Required**

* Bachelor's degree.

**Preferred**

* Master's degree or PhD and JD is highly desirable.

WORK EXPERIENCE

**Required**

* 5 years of relevant experience.
* 3 years of management experience.

**Preferred**

* 10 years of professional experience.
* 3 years in a direct leadership role with evidence of successful recruiting, evaluating, professionally developing, and retaining professionals.
* Experience in a research environment required in relevant areas.
* Prior military service.
* Experience with export control regulations and successfully leading export control programs.

ROLE SPECIFIC LICENSING AND REQUIREMENTS

**Required**

* Must be a U.S. citizen.
* Must be able to receive Defense Counterintelligence and Security Agency (DCSA) FSO possessing certification.
* Ability to obtain (if not already a certified Facility Security Officer (FSO)), all Defense Counterintelligence Security Agency FSO Program Management courses within 6 months of hire.
* Ability to obtain national security clearance at the level of the university's facility security clearance, including a willingness to take a polygraph test.

SKILLS

**Required**

* Proficient communication skills.
* Ability to lead/manage others.
* Effective leadership skills.
* Maintains a high degree of professionalism.
* Demonstrates time management and priority setting skills.
* Ability to work within tight time frames and meet strict deadlines.
* Possesses flexibility to work in a fast paced, dynamic environment.
* Ability to drive multiple projects to successful completion.
* Effective interpersonal skills.
* Excellent organizational skills.
* Highly thorough and dependable.
* Demonstrates a high level of accuracy, even under pressure.
* Strong verbal communication and listening skills.
* Effective conflict management skills.
* Maintains composure under pressure.
* Builds and manages effective teams.
* Instills commitment to organizational goals.

**Preferred**

* Strong knowledge of using government systems including NISS, DISS, SWFT, NBIS, eAPP, and Fieldprint. Working knowledge of the National Industrial Security Program (NISPOM) and Department of Defense regulations.
* Knowledge of business theory, business processes, management, budgeting, and business office operations.
* Demonstrated ability to recruit, evaluate, professionally develop, and retain high functioning professionals.
* Knowledge of federal regulations and university policies concerning information that has restrictions on dissemination, whether due to federal law or regulation, or contractual obligation. Knowledge of DOD Manual 5220.22-M or 32CFR117, the National Industrial Security Operating Manual (NISPOM) and familiarity with Export Control regulations (ITAR, EAR and OFAC). Must have some technical knowledge and an understanding of intellectual property.
* Thorough knowledge and ability to apply all relevant Federal, state, and university regulations, policies, and federal guidance documents. Thorough knowledge of and experience implementing appropriate regulations including the Department of State, Department of Commerce, Defense Counterintelligence Security Agency, Department of Defense, and the Department of Justice including but not limited to NISPOM and ITAR.
* Demonstrated in-depth knowledge of federal laws and regulations (NISPOM, etc.) pertaining to government industrial security programs, including knowledge of controlled material management and federal contract requirements.
* Facility security experience.
* Demonstrated ability to independently research, interpret, develop, and implement written policies and practices for a National Industrial Security Program.
* Demonstrated self-discipline and sound, independent judgment completing complex assignments. Proven ability to perform independently and with minimal direction. Demonstrated skill in organizing and setting priorities and accomplishing tasks in an environment with constantly changing priorities.
* Demonstrated ability to compile, review and analyze information/data, and to recommend alternatives. Demonstrated ability to adapt, implement, provide input into, and evaluate new procedures, systems, and processes.
* Demonstrated ability to develop training material and to provide individual training as appropriate and required for indoctrinations, advance security and travel briefings, debriefings, annual required trainings (SF-312, NATO, COMSEC, initial, insider threat, annual, etc.).
* Proven ability to maintain confidentiality and exercise discretion.
* Knowledge of the NIST SP 800-53, NIST SP 800-57 and the NIST SP 800-171/172A.
* Knowledge of Restricted Area (RA) and SCIF Standards as well as Intelligence Community Directive 705.

**Working Conditions and Demands**

This role requires the ability to effectively communicate and to operate a computer and other standard office productivity equipment. The position involves sedentary work as well as periods of time moving around an office environment and the campus. The person in this role must be able to perform the essential functions with or without an accommodation.

**Work Location**

Bloomington, Indiana

This position is eligible for remote work or to work a hybrid schedule (mix between remote or in-person work), subject to change based on university policy and business needs.

This position is being managed by IU's Executive Recruiting team. For questions related to this search or to nominate a candidate for this role, please email exesrch@iu.edu. Emails to this inbox are treated as confidential.

**Benefits Overview**

For full-time staff employees, Indiana University offers a wide array of benefits including:

* Multiple plan options for medical insurance
* Dental insurance
* Health Savings Account with generous IU contribution
* Life insurance, LTD, and AD&D options
* Base retirement plan contribution from IU, subject to vesting
* Additional supplemental retirement plan options
* Tuition benefit for IU classes
* 10 paid holidays per year
* Generous Paid Time Off
* Paid Parental Leave
* Employee Assistance Program (EAP)

Learn more about our benefits by reviewing our online [Benefits Brochure](https://hr.iu.edu/pubs/books/IU-benefits_broch.pdf).

**Job Classification**

Career Level: Senior Executive

FLSA: Exempt

Job Function: Engineering, Trades & Facility

Job Family: Facility Management

[Click here to learn more about Indiana University's Job Framework.](https://hrms.indiana.edu/psp/PH1PRD_PUB/EMPLOYEE/HRMS/c/IU_JC_COMPARE.IU_JC_COMPARE.GBL)

**Posting Disclaimer**

This posting is scheduled to close at 11:59 pm EST on the advertised Close Date. This posting may be closed at any time at the discretion of the University, but will remain open for a minimum of 5 business days. To guarantee full consideration, please submit your application within 5 business days of the Posted Date.

If you wish to include a cover letter, you may include it with your resume when uploading attachments.

**Equal Employment Opportunity**

Indiana University is an equal employment and affirmative action employer and a provider of ADA services. All qualified applicants will receive consideration for employment based on individual qualifications. Indiana University prohibits discrimination based on age, ethnicity, color, race, religion, sex, sexual orientation, gender identity or expression, genetic information, marital status, national origin, disability status or protected veteran status. Indiana University does not discriminate on the basis of sex in its educational programs and activities, including employment and admission, as required by Title IX. Questions or complaints regarding Title IX may be referred to the U.S. Department of Education Office for Civil Rights or the university Title IX Coordinator. [See Indiana University’s Notice of Non-Discrimination here which includes contact information](https://policies.iu.edu/policies/ua-01-equal-opportunity-affirmative-action/index.html).

**Campus Safety and Security**

The Annual Security and Fire Safety Report, containing policy statements, crime and fire statistics for all Indiana University campuses, is [available online](http://protect.iu.edu/police-safety/annual-reports/index.html). You may also request a physical copy by emailing IU Public Safety at [iups@iu.edu](mailto:iups@iu.edu) or by visiting IUPD.