CHICAGO STATE UNIVERSITY

1867

Chicago State University (CSU) Foreign Government Interference (FGI) and Research Security Policy

Effective: September 30, 2026

1) Introduction 2
2) Applicability 2
3) Definitions 3
4) Policy 3
5) Disclosure Requirements 4
6) Review of Disclosures 5
7) Foreign Talent Recruitment Programs 11
8) International Collaborations and Foreign Components 11
9) International Travel 12
10) Research Security Training 12
11) Cybersecurity and Protection of Research Information 13
12) Export Controls 13
13) Reporting Suspected Research Security Concerns 13
14) Subrecipient and Collaborator Requirements 14
15) Records and Documentation 14
16) Noncompliance, Corrective Actions, and Remedies 14
17) Related Policies and Resources 15
18) Public Accessibility of the FGI Policy and Research Security by Senior/Key Personnel 15
19) Point Of Contact 17

1) Introduction

Chicago State University ("CSU" or "the University") is committed to maintaining an open, collaborative, and internationally engaged research and scholarly environment while protecting the integrity, security, and transparency of the University's research enterprise.

International collaboration, foreign partnerships, visiting scholars, international travel, and access to global expertise are important components of research, education, and scholarly activity. CSU does not seek to discourage legitimate international collaboration or to restrict research or scholarly activity based on an individual's national origin, citizenship, ethnicity, or other protected characteristic.

At the same time, federal agencies have identified risks associated with inappropriate foreign government interference and exploitation of federally supported research. These risks may include undisclosed research support or affiliations, conflicts of commitment, improper participation in foreign talent recruitment programs, unauthorized transfer of research data or intellectual property, inappropriate access to confidential information, and other activities that may compromise the integrity or security of research.

This policy establishes CSU's framework for identifying, disclosing, evaluating, and mitigating risks associated with foreign government interference and research security. The policy is intended to support compliance with applicable federal laws, regulations, sponsor requirements, and research security guidance, including National Security Presidential Memorandum 33 (NSPM-33), the CHIPS and Science Act of 2022, Office of Science and Technology Policy (OSTP) guidance, and applicable requirements of federal research agencies.

The University recognizes that research security and foreign government interference requirements are evolving. This policy therefore establishes institutional expectations while allowing the University to implement additional procedures and requirements as required by federal agencies, sponsors, or applicable law.

2) Applicability

This policy applies to CSU faculty, staff, students, postdoctoral researchers, visiting scholars, and other individuals who participate in research or sponsored activities when they are subject to federal or University research security requirements.

Additional requirements may apply to individuals who:

- participate in federally funded research and development;
- are identified by a federal research agency as a covered individual or senior/key personnel;
- submit or participate in applications for federal research funding;
- receive or administer federal research awards;
- participate in international research collaborations or foreign components;
- engage in Institution-related international travel;
- access research data, intellectual property, controlled technologies, or other sensitive research information; or
- participate in activities subject to federal research security, export control, or foreign influence requirements.

Where a federal sponsor establishes requirements that are more restrictive than this policy, the sponsor's requirements will apply.

3) Definitions

For the purpose of these policies and procedures, the following definitions apply:

Foreign Entity means an organization, institution, government, business, or other legal entity located outside the United States or otherwise organized under the laws of a foreign country.

Foreign Government means the national, regional, provincial, local, or equivalent government of a country other than the United States.

Foreign Government Interference means actions by, or undertaken on behalf of, a foreign government or foreign entity that improperly influence, compromise, exploit, misappropriate, or otherwise threaten the integrity, security, or conduct of University research or scholarly activities.

Research Security means safeguarding the research enterprise against the misappropriation of research and development, inappropriate foreign government interference, unauthorized disclosure or transfer of research information, cybersecurity threats, and other activities that may harm the integrity or security of federally supported research.

Foreign Component means the performance of a significant scientific element or segment of a federally supported research project outside the United States, either by the recipient or by a researcher employed by a foreign organization, as defined by the applicable federal sponsor.

Foreign Talent Recruitment Program (FTRP) means a program, position, or activity sponsored by a foreign government or foreign entity that seeks to recruit researchers or other individuals to participate in research or related activities. Participation in an FTRP is not inherently prohibited; however, certain programs may be subject to federal disclosure, certification, or other requirements.

Malign Foreign Talent Recruitment Program (MFTRP) means a foreign talent recruitment program meeting the definition established by applicable federal law, including the CHIPS and Science Act of 2022, or applicable federal sponsor requirements.

Covered Individual means an individual who meets the definition established by applicable federal law or federal research agency requirements and who is subject to research security requirements under a federal research award or application.

Senior/Key Personnel means individuals designated by the applicable federal research agency as having responsibility for the design, conduct, or reporting of research or otherwise designated as senior/key personnel under the agency's requirements.

Other Support means resources made available to an individual in support of and/or related to all of the individual's research endeavors, as defined by the applicable federal sponsor.

International Travel means travel outside the United States undertaken in connection with University business, including research, teaching, conferences, meetings, or other scholarly activities.

4) Policy

CSU is committed to protecting the integrity and security of its research enterprise while preserving legitimate international collaboration and academic freedom.

The University will:

1. Maintain and periodically update a research security program consistent with applicable federal requirements.
2. Provide guidance and resources to members of the CSU research community regarding foreign government interference, research security, disclosure requirements, international collaboration, and related federal requirements.
3. Provide required or appropriate research security training, including training addressing foreign interference, cybersecurity, international collaboration, disclosure obligations, conflicts of interest and commitment, and appropriate use of federal research funds.
4. Provide export control training and guidance to individuals whose research or scholarly activities are subject to export control requirements.
5. Provide foreign travel security guidance and, when required, training for covered individuals.
6. Maintain appropriate systems for required disclosure of foreign affiliations, support, activities, and relationships.
7. Maintain procedures for reporting and addressing suspected research security concerns or violations.
8. Coordinate with federal sponsors and other University offices as necessary to evaluate and mitigate identified research security risks.
9. Protect research data, intellectual property, confidential information, controlled information, and other research resources from unauthorized access, disclosure, transfer, or use.
10. Apply this policy in a manner that does not discriminate on the basis of national origin, citizenship, ethnicity, race, or other protected characteristics.

The University recognizes that foreign collaboration and international engagement are not inherently problematic. Risk assessments and compliance actions will be based on relevant activities, relationships, disclosures, contractual obligations, sponsor requirements, and other objective factors.

5) Disclosure Requirements

Individuals subject to this policy are responsible for providing complete and accurate disclosures of foreign research support, affiliations, activities, relationships, and other information required by CSU and applicable federal sponsors. Financial interests must also be disclosed in accordance with CSU's Conflict of Interest Policy and applicable federal requirements. Depending on the applicable requirements, disclosures may include:

- foreign research support;
- foreign financial support or compensation;
- foreign employment or appointments;
- academic, professional, or institutional affiliations with foreign entities;
- foreign research collaborations;
- foreign components of federally funded research;
- in-kind research resources, including equipment, laboratory space, personnel, materials, or other resources;
- participation in foreign talent recruitment programs;
- foreign-sponsored or reimbursed travel;
- other resources made available in support of an individual's research;
- contracts, agreements, or other commitments with foreign entities; and
- other information required by the applicable federal sponsor.

Investigators must make disclosures in the format, system, and timeframe required by CSU and the applicable funding agency.

For NIH-funded research, senior/key personnel must comply with NIH requirements for disclosure of Other Support, foreign components, and applicable financial conflicts of interest. NIH states that full transparency regarding research support, foreign components, and financial conflicts of interest is required throughout the lifecycle of an NIH award. For NSF, Higher education institutions receiving NSF funding must report financial support linked to foreign countries of concern. Applicants, recipients, and subrecipients of the Department of Energy must submit transparency disclosures of foreign connections. The Department of Defense directs 30 U.S. universities to audit and report on foreign research collaborations by reviewing notices detailed in DoD Orders 30 Universities to Audit Foreign Research Collaborations.

Individuals should consult the Office of Grants and Research Administration when they are uncertain whether a foreign relationship, activity, resource, or commitment must be disclosed.

6) Review of Disclosures

CSU will review disclosures and other information that may indicate a potential foreign government interference or research security concern. The purpose of the review is to determine whether the activity, relationship, or information disclosed is consistent with applicable federal requirements, sponsor requirements, and University policies and whether additional action or mitigation is necessary.

A. Designated Official

The Associate Provost for Grants and Research Administration (APGRA) will serve as the University's Designated Official (DO) for purposes of reviewing disclosures and research security concerns under this policy.

The DO is responsible for:

1. Reviewing disclosures and information relevant to foreign government interference and research security;
2. Determining whether additional information is necessary to complete the review;
3. Coordinating, as appropriate, with other University offices with relevant expertise;
4. Determining whether a disclosed activity or relationship is subject to additional federal, sponsor, or University requirements;
5. Determining whether a research security concern exists and whether mitigation or corrective action is necessary;
6. Documenting the University's review and determination;
7. Communicating determinations and required actions to the affected individual; and
8. Coordinating with the applicable federal sponsor when reporting or other action is required.

If the APGRA has an actual or perceived conflict of interest or conflict of commitment related to a matter under review, the APGRA will recuse themselves from the review and determination. In such circumstances, the Provost, or another University official designated by the Provost, will serve as the DO for that matter. The recusal and designation of an alternate DO will be documented.

The DO may consult with subject matter experts or other University officials as necessary. Such consultation may include representatives from the Office of General Counsel, Information Technology, Global Engagement, Export Controls, Human Resources, Conflict of Interest/Conflict of Commitment, Sponsored Programs, or other appropriate offices.

B. Initial Review of Disclosures

Disclosures required under this policy will be reviewed by the DO or by University personnel designated by the DO. The DO retains responsibility for final determinations under this policy unless responsibility has been formally delegated in writing. The initial review will determine:

1. Whether the disclosure is complete and sufficiently detailed to permit review;
2. Whether the disclosed activity or relationship is subject to federal, sponsor, or University disclosure requirements;
3. Whether the activity involves a foreign entity, foreign government, foreign institution, or foreign individual;
4. Whether the activity involves foreign research support, a foreign appointment or affiliation, a foreign component, foreign-sponsored travel, a foreign talent recruitment program, or another activity requiring additional review;
5. Whether the activity has been appropriately disclosed through all required University and federal reporting mechanisms;
6. Whether the activity creates an actual, potential, or apparent conflict of interest or conflict of commitment;
7. Whether the activity creates scientific, budgetary, or commitment overlap with CSU research or sponsored activities;
8. Whether the activity may create risks involving research data, intellectual property, confidential information, controlled technology, cybersecurity, or other protected research resources; and
9. Whether additional review, disclosure, sponsor notification, or mitigation is necessary.

The DO may request supporting documentation from the Investigator or other appropriate University personnel. Supporting documentation may include, but is not limited to:

- contracts or agreements;
- appointment or employment letters;
- grant or award documentation;
- descriptions of foreign research activities;
- documentation of foreign research support;
- information regarding foreign talent recruitment programs;
- travel documentation;
- copies of disclosure forms submitted to federal agencies;
- information regarding research collaborations or foreign components;
- information regarding commitments of time and effort; and
- other documentation reasonably necessary to complete the review.

Investigators are expected to provide requested information completely and accurately and within the timeframe established by the DO.

C. Review of Relationship to University Research

When a disclosure or other information identifies a foreign activity or relationship involving an Investigator, the DO will evaluate whether the activity is related to the Investigator's CSU research or sponsored activities.

The DO may consider whether:

- the activity involves the same or substantially similar research as a CSU project;
- the foreign activity provides financial or other research support;
- the foreign activity involves the use of University resources;
- the foreign activity involves research personnel, students, facilities, equipment, data, or intellectual property associated with CSU;
- the activity creates overlapping commitments of time or effort;
- the activity creates scientific or budgetary overlap with a CSU or federally funded project;
- the activity involves a foreign component that has not been disclosed or approved;
- the activity involves a foreign talent recruitment program;
- the activity creates obligations that are inconsistent with the Investigator's responsibilities to CSU or a federal sponsor; or
- the activity otherwise creates a risk to the integrity, security, or appropriate stewardship of University or federally funded research.

The DO may consult with the Investigator when determining whether an activity is related to University research. Consultation with the Investigator does not relieve the Investigator of responsibility for providing complete and accurate disclosures.

D. Review of Potential Research Security Concerns

A research security concern may be identified through an Investigator disclosure, federal sponsor inquiry, internal review, audit, report from another University office, or other information available to the University.

When a potential research security concern is identified, the DO will conduct an initial assessment to determine:

1. The nature and scope of the concern;
2. Whether University or federally funded research is involved;
3. Whether the concern involves an undisclosed or inaccurately disclosed activity or relationship;
4. Whether the concern involves foreign research support, foreign employment or appointments, foreign components, foreign talent recruitment programs, or other foreign affiliations;
5. Whether the concern involves potential scientific, budgetary, or commitment overlap;
6. Whether the concern involves a conflict of interest or conflict of commitment;
7. Whether research data, intellectual property, confidential information, controlled technology, or other research resources may have been improperly accessed, transferred, disclosed, or used;
8. Whether applicable export control, cybersecurity, data security, or other requirements may have been violated; and
9. Whether immediate action is necessary to protect research, research funds, University resources, or individuals.

The DO may determine that no further action is necessary when the available information demonstrates that the activity is appropriately disclosed, permissible under applicable requirements, and does not present an identified research security concern. The determination will be documented.

E. Requests for Additional Information

If the information provided in a disclosure is incomplete or raises questions that cannot be resolved through the initial review, the DO may request additional information from the Investigator.

The request may include a deadline for response and may identify the specific information or documentation needed.

Failure to provide requested information may result in the matter being escalated for additional review and may constitute noncompliance with this policy when the Investigator is required to provide the information.

When appropriate, the DO may suspend review of a proposal, award, disclosure, or related activity until sufficient information is provided to determine compliance.

F. Determinations

Following review, the DO will make one of the following determinations, as appropriate:

1. No Concern Identified: The activity or relationship is appropriately disclosed and does not create an identified research security, compliance, conflict of interest, or conflict of commitment concern. No additional action is required beyond routine monitoring or reporting.

2. Disclosure or Documentation Correction Required: The activity itself is permissible, but the Investigator must correct or supplement a University or federal disclosure, provide additional documentation, or make another administrative correction.

3. Additional Review Required: The available information is insufficient to determine whether a research security concern exists, or the matter requires review by another University office, subject matter expert, or federal sponsor.

4. Mitigation Required: A research security concern has been identified that can be addressed through appropriate mitigation measures. The DO will establish or coordinate a written mitigation plan describing the actions required, the individual responsible for completing each action, and any applicable monitoring requirements.

5. Sponsor Notification or Approval Required: The activity requires notification to, disclosure to, or prior approval from the applicable federal sponsor. CSU will coordinate the required submission or communication with the sponsor.

6. Noncompliance Identified: The review identifies a violation of federal requirements, sponsor requirements, or University policy. The matter will be handled in accordance with Section 16 of this policy and any other applicable University policy.

7. Escalation Required: The matter presents significant or unresolved research security concerns, potential violations of law, or circumstances requiring institutional leadership or external review. The DO will refer the matter to the appropriate University officials and, when required, the applicable federal sponsor or governmental authority.

The DO will document the basis for the determination and any required actions.

G. Mitigation Measures

When a research security concern is identified but the underlying activity or relationship is not prohibited, CSU may implement mitigation measures designed to reduce or eliminate the identified risk.

Depending on the circumstances, mitigation measures may include:

1. Correcting or updating a disclosure;
2. Obtaining required sponsor approval;
3. Establishing a written management or mitigation plan;
4. Modifying the Investigator's role or responsibilities;
5. Removing or restricting access to certain research data, systems, facilities, equipment, or information;
6. Implementing additional cybersecurity or data security controls;
7. Requiring additional research security, export control, or cybersecurity training;
8. Requiring review of an agreement or contract by the appropriate University office;
9. Modifying or terminating a research activity or relationship when required;
10. Requiring additional monitoring or periodic reporting;
11. Restricting use of University or federally funded research resources; or
12. Taking other actions reasonably necessary to protect the integrity and security of the research.

The mitigation measures selected will be proportionate to the nature and severity of the identified concern.

H. Review Timelines

CSU will conduct reviews in a timely manner based on the nature of the disclosure or concern.

Prior to Award or Expenditure of Funds. When a research security concern is identified before a federal award is issued or before funds may be expended, the DO will review the matter before the applicable deadline and, when necessary, coordinate with the sponsor before CSU proceeds with the award.

New Investigator or New Disclosure During an Award. When a new Investigator joins a federally funded project or an existing Investigator reports a new activity or relationship during an award period, the DO will promptly review the disclosure and determine whether additional action is required.

Newly Identified Concern. When CSU becomes aware of a previously undisclosed or inaccurately disclosed activity or other potential research security concern during an award period, the DO will initiate a review promptly and determine whether interim measures, sponsor notification, correction of disclosures, or other action is necessary.

Federal Sponsor Inquiry. When a federal sponsor requests information regarding a disclosure or potential foreign interference concern, CSU will respond within the timeframe established by the sponsor.

Where federal law, regulation, or sponsor requirements establish a specific reporting or review deadline, the federal requirement will control.

I. Interim Measures

When the DO reasonably determines that an identified concern presents an immediate or significant risk to research security, the University may implement interim measures while the review is ongoing.

Interim measures may include temporarily restricting access to research data, systems, equipment, facilities, funds, or other resources; pausing a research activity; or taking other steps necessary to protect the research enterprise.

Interim measures are not a determination that an individual has violated this policy. They may be implemented when necessary to protect research while the University completes its review.

J. Communication of Determinations

The DO will communicate determinations and required corrective or mitigation actions to the Investigator in writing.

When a mitigation or corrective action is required, the written communication will identify, as appropriate:

- the concern or requirement identified;
- the action(s) required;
- the responsible individual or office;
- the deadline for completing the action;
- any required documentation;
- the monitoring process; and
- the consequences of failing to complete the required action.

The Investigator may request clarification regarding a determination or required action.

K. Monitoring and Follow-Up

CSU will monitor compliance with mitigation plans and other corrective actions for the duration necessary to address the identified concern.

The DO may request documentation demonstrating that required actions have been completed. Depending on the circumstances, the DO may also conduct periodic reviews to determine whether:

- required disclosures remain accurate and current;
- mitigation measures remain effective;
- changes in the Investigator's activities or relationships require additional review;
- additional sponsor reporting or approval is required; or
- the research security concern has been resolved.

When a mitigation plan is no longer necessary, the DO will document the conclusion of the monitoring period.

L. Federal Sponsor Coordination

When a disclosure or research security concern involves a federally funded project, CSU will comply with applicable sponsor reporting, disclosure, and prior-approval requirements.

The University may provide the federal sponsor with information necessary to evaluate compliance, including supporting documentation regarding foreign research support, foreign affiliations, foreign components, conflicts of interest or commitment, or other matters relevant to the award.

For NIH-funded research, CSU will follow NIH requirements for reporting and responding to concerns involving Other Support, foreign components, financial conflicts of interest, and other potential foreign interference. NIH's current process specifically contemplates institutional review of whether support was properly disclosed and whether scientific, budgetary, or commitment overlap, FCOI, or foreign-component issues are present.

M. Documentation of Review

Records will be maintained in accordance with Section 15 of this policy and applicable University and federal record-retention requirements.

7) Foreign Talent Recruitment Programs

CSU recognizes that foreign talent recruitment programs may support legitimate international research and academic collaboration.

However, individuals subject to federal restrictions may not participate in a Malign Foreign Talent Recruitment Program (MFTRP).

Covered individuals must disclose participation in foreign talent recruitment programs as required by federal agencies and CSU policy.

Individuals who are uncertain whether a particular program qualifies as an MFTRP should consult the Office of Grants and Research Administration before participating in the program or accepting associated compensation, appointments, or other benefits.

Where required by federal law or sponsor policy, covered individuals must certify that they are not participating in an MFTRP as part of the federal application or award process.

8) International Collaborations and Foreign Components

CSU supports international research collaboration that is conducted transparently and in accordance with applicable requirements.

Investigators are responsible for identifying and reporting foreign components and other international research activities when required by the applicable sponsor.

Before initiating a foreign component or other significant international research activity on a federally funded project, investigators must obtain any required sponsor approval. International collaborations must also be disclosed and reviewed by OGRA.

Investigators must also ensure that international collaborations comply with:

- applicable award terms and conditions;
- disclosure requirements;
- export control requirements;
- intellectual property and confidentiality requirements;
- applicable data security requirements;
- human subjects and animal research requirements;
- University agreements and contracting requirements; and
- other applicable federal, state, and University policies.

International visitors must not be placed in positions where they can access restricted or export-controlled research

without prior authorization.

For NIH-funded research, foreign components generally include significant scientific activities conducted outside the United States or involving a foreign organization or researcher. NIH requires appropriate disclosure and, where applicable, prior approval.

9) International Travel

Covered individuals who engage in international travel in connection with University business must comply with applicable University travel reporting and security requirements.

Depending on the individual's role and the purpose of the travel, requirements may include:

- reporting international travel through the University's designated travel reporting system;
- completing required foreign travel security training;
- protecting University devices, data, and research information while traveling;
- complying with export control requirements;
- following University cybersecurity requirements;
- reporting loss or compromise of University devices or information; and
- following sponsor-specific travel requirements.

International travel for legitimate academic, research, or professional purposes is not prohibited by this policy.

10) Research Security Training

CSU will provide research security training to individuals subject to federal research security requirements.

Training may address:

- foreign government interference and research security;
- disclosure of Other Support and foreign affiliations;
- conflicts of interest and commitment;
- foreign talent recruitment programs;
- cybersecurity and protection of research information;
- international collaboration;
- appropriate use of federal research funds;
- export controls;
- foreign travel security; and
- reporting suspected research security concerns.

Covered individuals must complete required training within the timeframe established by federal requirements and University procedures. CSU will monitor completion of required research security training and may take appropriate administrative action when required training has not been completed within the applicable timeframe.

Additional training may be required when:

- an individual becomes subject to research security requirements;
- federal requirements change;
- research is used in dual-use applications (both civilian and military);
- CSU revises this policy or related procedures;
- an individual begins participation in a federally funded project requiring training; or

- CSU determines that additional training is necessary to address a compliance concern.

11) Cybersecurity and Protection of Research Information

CSU will maintain cybersecurity practices designed to protect research data, systems, intellectual property, controlled information, and other research resources.

Researchers and other individuals subject to this policy are expected to:

- follow University information security requirements;
- use University-approved systems for protected research information when required;
- protect passwords, authentication credentials, devices, and research accounts;
- appropriately secure research data and intellectual property;
- avoid unauthorized transfer or disclosure of research information;
- promptly report suspected cybersecurity incidents; and
- comply with sponsor-specific information security requirements.

Additional safeguards may be required for research involving controlled, sensitive, export-controlled, proprietary, personally identifiable, or otherwise restricted information.

12) Export Controls

Individuals engaged in research or scholarly activities involving export-controlled technology, software, equipment, technical information, or other regulated items must comply with applicable U.S. export control laws and University policies.

Export control requirements may apply to international collaborations, foreign persons, international travel, shipping or transferring research materials or technology, and access to controlled technical information.

Researchers should contact the University's designated export control office before transferring controlled technology, technical information, software, equipment, or other regulated items to a foreign person or foreign country.

This policy does not replace CSU's separate Export Control Policy or related procedures.

13) Reporting Suspected Research Security Concerns

Members of the CSU research community are expected to report suspected violations of this policy or applicable research security requirements.

Examples may include:

- undisclosed foreign research support;
- undisclosed foreign appointments or affiliations;
- undisclosed foreign components;
- suspected participation in an MFTRP;
- unauthorized transfer of research data or intellectual property;
- inappropriate access to confidential research information;
- suspected cybersecurity compromise;
- undisclosed conflicts of commitment;
- inaccurate or incomplete federal disclosures; or
- other activities that may compromise research security or violate federal award requirements.

Reports should be made to the APGRA at Edmundo.garcia@csu.edu.

CSU will evaluate reports in accordance with applicable University policies and procedures and will refer matters to federal sponsors or other authorities when required.

Individuals who make good-faith reports of potential violations will be protected from retaliation to the extent provided by applicable law and University policy.

14) Subrecipient and Collaborator Requirements

When federal funds are provided to a subrecipient or collaborator, CSU will establish appropriate requirements addressing research security, disclosures, conflicts of interest and commitment, foreign components, and other applicable federal requirements.

Subrecipient agreements may require the subrecipient to:

- comply with applicable federal research security requirements;
- provide required disclosures;
- certify compliance with applicable requirements;
- report research security concerns to CSU;
- provide information necessary for CSU to meet sponsor reporting requirements; and
- comply with additional terms imposed by the federal sponsor.

The specific requirements applicable to a subrecipient will depend on the award, federal sponsor, and nature of the subrecipient relationship.

15) Records and Documentation

CSU will maintain records necessary to demonstrate compliance with this policy and applicable federal requirements.

Records may include:

- required disclosures;
- training completion records;
- international travel records;
- certifications;
- research security reviews;
- mitigation plans;
- reports of suspected violations;
- documentation of investigations and corrective actions; and
- correspondence with federal sponsors regarding research security matters.

Records will be maintained in accordance with applicable federal requirements, University record-retention policies, and sponsor terms and conditions.

16) Noncompliance, Corrective Actions, and Remedies

Failure to comply with this policy may result in corrective or disciplinary action, consistent with applicable University policies, employment agreements, federal requirements, and law.

Depending on the nature and severity of the violation, corrective actions may include:

- additional training;
- correction of inaccurate or incomplete disclosures;
- development of a research security mitigation plan;

- restrictions on access to research information or resources;
- modification of research activities;
- removal from a research project;
- restrictions on participation in federally funded research;
- suspension or termination of research activities;
- disciplinary action under applicable University procedures; and/or
- notification to the applicable federal sponsor or other governmental authority.

Federal agencies may impose additional remedies for noncompliance, including specific award conditions, restrictions on funding, recovery of funds, suspension, termination, or referral for suspension or debarment. NIH's current procedures, for example, provide for actions ranging from requests for additional information and mitigation to restrictions on funds or other grants-management actions depending on the circumstances.

Nothing in this policy limits the University's obligation to take corrective action or report matters when required by federal law, regulation, or award terms.

17) Related Policies and Resources

This policy should be read in conjunction with applicable CSU policies and procedures, including:

- Conflict of Interest Policy;
- Conflict of Commitment Policy;
- Export/Import Control Policy;
- Information Security/Cybersecurity Policy;
- Sponsored Programs policies and procedures;
- International Travel policies and procedures;
- Intellectual Property Policy;
- Research Integrity and Misconduct policies;
- Human Subjects Research policies;
- Data Security and Privacy policies; and
- applicable federal sponsor requirements.

Relevant federal resources include:

- National Security Presidential Memorandum 33 (NSPM-33);
- OSTP Guidelines for Research Security Programs at Covered Institutions;
- CHIPS and Science Act of 2022;
- NIH Foreign Interference guidance;
- NIH Other Support requirements;
- NIH Foreign Component requirements;
- NIH research security training requirements;
- NSF research security guidance and disclosure requirements; and
- applicable federal export control requirements.

Federal requirements may change. Researchers are responsible for following the requirements applicable to their specific award or research activity.

18) Public Accessibility of the FGI Policy and Research Security by Senior/Key Personnel

A. Public Availability of the Policy

CSU will make this Foreign Government Interference and Research Security Policy publicly available on the University's website.

The University will review the policy periodically and update it as necessary to reflect changes in applicable federal laws, regulations, federal agency requirements, and University procedures.

The publicly available version of the policy will identify the University's general requirements and responsibilities related to foreign government interference and research security. Detailed internal procedures, security controls, review materials, and other information that could compromise research security or University operations may be maintained separately and may not be publicly available.

B. Public Information Regarding the Research Security Program

CSU will make available appropriate information describing its research security program, including, as applicable:

- the purpose and scope of the University's research security program;
- the University's commitment to protecting research integrity while supporting legitimate international collaboration;
- the University's general research security requirements;
- required research security training;
- foreign travel security requirements;
- cybersecurity and research data security expectations;
- export control requirements;
- disclosure requirements related to foreign research support, affiliations, activities, and relationships;
- requirements regarding foreign talent recruitment programs;
- procedures for reporting suspected research security concerns; and
- the appropriate University offices or officials to contact with questions regarding research security.

The University may provide additional public information regarding federal research security requirements when appropriate.

C. Confidentiality and Protection of Information

CSU will protect confidential, proprietary, personal, security-sensitive, and otherwise restricted information obtained or created as part of a research security review to the extent permitted by applicable law.

Information related to an individual's foreign affiliations, research support, financial interests, conflicts of interest or commitment, research activities, or research security review will not be made publicly available solely because it has been disclosed to the University under this policy, unless disclosure is required by applicable law, regulation, federal sponsor requirements, or other legal obligation.

CSU will take reasonable steps to limit access to research security records to individuals with a legitimate institutional need to review the information.

Nothing in this section prevents CSU from providing information to a federal sponsor, governmental authority, auditor, or other authorized entity when disclosure is required by law, regulation, award terms, or an official request.

D. Public Disclosure of Individual Information

CSU will not routinely publish individual Investigators' foreign affiliations, foreign research support, travel, participation in international collaborations, or other information submitted under this policy.

Where federal law or a federal sponsor specifically requires public disclosure of information concerning an Investigator, financial interest, research support, or other matter, CSU will provide the information in the manner and timeframe required by the applicable authority.

Any public disclosure required by a federal sponsor will be limited to the information required by the applicable requirement.

E. Requests for Information

Requests for information concerning CSU's research security program or compliance with this policy should be directed to the Office of Grants and Research Administration.

Requests for records will be handled in accordance with applicable federal and state law, University policies, public-records requirements, privacy protections, and restrictions applicable to confidential, proprietary, export-controlled, or security-sensitive information.

Nothing in this policy creates a right to access information that is otherwise exempt from disclosure under applicable law or University policy.

19) Point Of Contact

Questions regarding this policy, research security requirements, foreign government interference, required disclosures, or related federal requirements should be directed to:

Contact:

Edmundo Garcia-Solis
Associate Provost for Grants and Research Administration
Chicago State University
9501 South King Dr. ADM 303
Chicago IL, 60628
edmundo.garcia@csu.edu

Researchers should contact the Office of Grants and Research Administration before entering into an unfamiliar foreign research relationship, accepting foreign research support, participating in a foreign talent recruitment program, establishing a foreign component on a federally funded project, or transferring potentially controlled research information or technology internationally.