Arizona State University Addendum Subrecipient Commitment Form: Cybersecurity and Research Security

March 2026

Certification Statements (Select one of the certifications)

⭘ **Currently Compliant** - The Subrecipient represents and certifies that, as of the date of this certification, it maintains cybersecurity and research security controls that are consistent with and sufficient to comply with all applicable federal, sponsor, and prime recipient requirements for the proposed project, including but not limited to requirements related to data protection, disclosure, export controls, conflicts of interest, and research security.

⭘ **Assurance of Just-In-Time Compliance** - The Subrecipient represents and certifies that, prior to receipt of a subaward, it will implement cybersecurity and research security controls that are consistent with and sufficient to comply with all applicable federal, sponsor, and prime recipient requirements for the proposed project, including but not limited to requirements related to data protection, disclosure, export controls, conflicts of interest, and research security.

Acknowledgment

☐ The Subrecipient acknowledges that failure to maintain or timely implement required cybersecurity and research security controls described above may impact its ability to participate in the award and may require additional conditions or mitigation measures.

A. Information Security Program

☐ Subrecipient maintains and implements a written Information Security Program that includes documented policies, procedures, and controls designed to safeguard all data types involved in the proposed scope of work and to comply with applicable federal, sponsor, and prime recipient requirements appropriate to the risk level.

B. Federal Cybersecurity Compliance (if applicable to the project)

NOTE: Per the National Archives CUI Registry glossary, Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to law, regulation, or government-wide policy.

If the proposed scope of work involves access to, storage of, transmission of, or processing of Controlled Unclassified Information (CUI):

Does your organization currently maintain and implement a Controlled Unclassified Information (CUI) security environment that is designed to comply with applicable requirements of NIST SP 800-171?

⭘ Yes
⭘ No

Arizona State University Addendum Subrecipient Commitment Form: Cybersecurity and Research Security

March 2026

☐ If **No, Subrecipient acknowledges** that a fully compliant CUI environment must be implemented before any CUI can be accessed or processed under this award.

If **Yes, the environment [select all that apply]**

☐ Has a written System Security Plan.
☐ Has been assessed by a third party
☐ If no third-party assessment, an internal NIST SP 800-171 assessment has been completed

Please provide the following for your CUI environment:

CAGE Code: _____
SPRS Score: _____

C. Incident Response & Reporting

☐ **Written Incident Response Plan** - The Subrecipient maintains and implements a written Incident Response Plan that includes procedures for identifying, responding to, mitigating, and documenting cybersecurity incidents impacting information or systems related to the proposed scope of work.

☐ Capability to support sponsor-specific incident reporting requirements - The Subrecipient has the capability to comply with applicable sponsor and prime recipient incident reporting requirements, including timely notification, cooperation in investigation and mitigation efforts, and provision of required documentation.

D. Export Controls

Export controls are U.S. federal laws and regulations (including ITAR/EAR/OFAC sanctions programs) that restrict the flow of certain materials, devices and technical information to foreign countries and to foreign nationals residing in the United States.

D.1. Project-Specific Determination

Based on the proposed scope of work:

Does the Subrecipient anticipate that the project will involve access to, receipt of, generation of, or dissemination of export-controlled material, data, software, or items?
🔘 Yes
🔘 No

D.2. Institutional Export Control Program

Arizona State University Addendum Subrecipient Commitment Form: Cybersecurity and Research Security

March 2026

Does the Subrecipient maintain a compliant export control program (ITAR/EAR/OFAC, as applicable)?

⭘ Yes
⭘ No

If **Yes**:
☐ Provide a weblink to Subrecipient's export (trade) compliance guidance (if available):_____

E. Research Security

Covered Institution Determination (OSTP 2024)

Is the Subrecipient *a "Covered Institution" as defined in the OSTP Guidelines for Research Security Programs at Covered Institutions (2024)?*

⭘ Yes
⭘ No

If Yes (Covered Institution), respond to E.2 and E.4.

If No (Not a Covered Institution), respond to E.3 and E.4.

Research Security Program

E.2. Does the Subrecipient maintain and implement a Research Security Program that meets OSTP 2024 requirements?

⭘ Yes
⭘ No

E.3. Does the Subrecipient maintain a Research Security Program consistent with NSPM-33 and related guidance to identify and manage risks to research security and integrity?

⭘ Yes
⭘ No

E.4. Does the Subrecipient provide Research Security training to relevant personnel involved in the proposed scope of work?

⭘ Yes
⭘ No

If **Yes**, training covers (check all that apply):
☐ Export controls
☐ Undue foreign influence
☐ Conflicts of interest/commitment

Arizona State University Addendum Subrecipient Commitment Form: Cybersecurity and Research Security

March 2026

- ☐ Research security awareness
- ☐ Foreign travel
- ☐ HIPAA for Covered Entity Employees – when applicable
- ☐ HIPAA for Researchers – when applicable

F. Disclosure & Transparency

Will any foreign persons (including foreign nationals, foreign institutions, or personnel with foreign affiliations) participate in the proposed project?

- ☐ Yes
- ☐ No

Does the Subrecipient have processes and/or policies in place to ensure compliance with applicable sponsor disclosure requirements?

- ☐ Yes
- ☐ No

If **Yes**, Check all that apply;

- ☐ Compliance with sponsor requirements for current and pending support
- ☐ Disclosure of foreign affiliations, appointments, and resources
- ☐ Disclosure of in-kind support and external research support

G. Foreign Influence & Malign Foreign Talent Programs

☐ The Subrecipient certifies that no senior/key personnel or other personnel participating in the proposed project are currently participating in a Malign Foreign Talent Recruitment Program as defined in 42 U.S.C. § 19237 and related federal guidance.

☐ The Subrecipient maintains policies or procedures designed to identify, disclose, and manage risks related to foreign influence, including risks arising from foreign affiliations, funding, or talent recruitment activities.

H. Points of Contact

The Subrecipient designates the following individuals as points of contact for cybersecurity, information security, and research security matters related to the proposed project. The individuals listed should have appropriate authority or subject-matter responsibility for the identified areas.

H.1 Information Technology & Cybersecurity Points of Contact

Primary IT/Cybersecurity Contact

- Name:
- Title (e.g., CISO, Director of Information Security, IT Compliance Manager):
- Email / Phone:

Arizona State University Addendum Subrecipient Commitment Form: Cybersecurity and Research Security

March 2026

- Areas of Responsibility (Select all that apply):
  - ☐ Information Security Program
  - ☐ CUI / NIST SP 800-171 Compliance
  - ☐ Incident Response & Reporting

Secondary / Technical IT Contact (if applicable)

- Name:
- Title:
- Email / Phone:
- Areas of Responsibility (Select all that apply):
  - ☐ System Security Plans (SSPs)
  - ☐ Security Assessments
  - ☐ Technical Remediation

H.2 Research Security & Compliance Point of Contact

Research Security Contact

- Name:
- Title (e.g., Research Security Officer, Director of Research Compliance):
- Office/Department:
- Email / Phone:
- Areas of Responsibility (Select all that apply):
  - ☐ Research Security Program (OSTP 2024 / NSPM-33)
  - ☐ Export Controls (ITAR/EAR/OFAC)
  - ☐ Disclosure & Transparency Requirements
  - ☐ Foreign Influence & Talent Program Compliance
  - ☐ Research Security Training