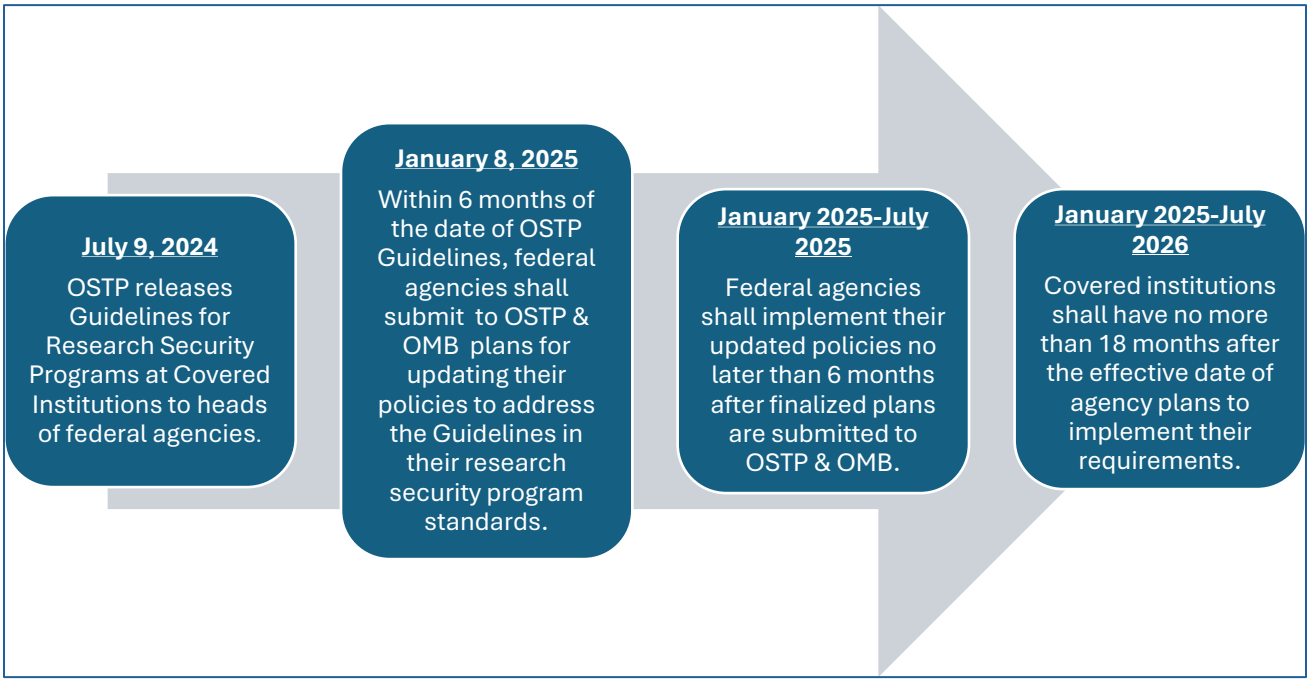
Overview of OSTP Guidelines for Research Security Programs at Covered Institutions

Summary Analysis: OSTP published its long-awaited research security program guidelines on July 9, 2024. The Guidelines confirm the four mandatory program elements necessary for a compliant research security program: (1) Cybersecurity; (2) Foreign Travel Security; (3) Research Security Training; and (4) Export Control Training. They also provide an implementation timetable for federal agencies and institutions:

Implementation Timetable:



The Guidelines represent an improvement from the prior draft standards in certain respects and provide greater flexibility for institutions in developing institutional research security programs. Notably, the Guidelines incorporate a number of existing statutory and policy definitions, which promote consistency. The Guidelines also include a clear definition for "Covered Institution" that cites concrete reference points institutions can use to determine if they meet the financial threshold for establishing a research security program. Importantly, the Guidelines state that they provide "standardized requirements," and they encourage agencies to consider administrative burden and impacts on less-resourced institutions in developing implementation plans.

However, despite the Guidelines' call for cross-agency consistency and agency consideration of administrative burden in developing implementation plans, they also afford significant latitude to agencies in their interpretation and implementation. Specifically, the Guidelines set forth a clear path that agencies can follow to adopt *different* requirements. Further, they contain no specific means by which administrative burden (particularly burden on lesser resourced institutions) must be measured or limited.

Finally, the Guidelines contain several provisions that cannot be fully assessed because they require significant further development by the federal government. For example, the Guidelines' cybersecurity standards reference a National Institute of Standards and Technology (NIST) resource that has not yet been published. Additionally, the institutional certification system is undefined, and the federal government resource that institutions may use in providing mandated foreign travel security training is not yet developed.

Background: The Guidelines were issued to fulfill the mandates of National Security Presidential Memorandum 33 (NSPM-33) and relevant provisions of the CHIPS and Science Act of 2022. The Guidelines present a "standardized requirement" for "uniform implementation" across federal agencies.

The Guidelines state that the overarching purpose of federal research security efforts "is to make sure that institutions of higher education (IHE) and other research institutions recognize the altered global landscape and fulfill their responsibilities as the first line of defense against improper or illicit activity." They also note that actions that researchers were encouraged to take a decade ago, including "collaborations with the PRC" are now recognized as presenting risks.

Guidelines as a Baseline: The Guidelines state that federal research agencies are permitted "to develop additional requirements for the research security programs" in addition to the four required program elements. Such additional requirements must be reviewed and approved by OMB and OIRA. Federal research funding agencies are instructed to limit additional requirements to the following circumstances:

- When required by statute, regulation, or executive order or action.
- When more stringent protections are necessary to protect classified information, export-controlled technologies, or other legally protected matters.
- When there are "other compelling agency-specific reasons consistent with legal authorities and mission of an individual agency and in coordination with OSTP."

When imposing additional requirements, the Guidelines instruct agencies to determine if concerns can be addressed at the award level. Further, agencies must also consider whether the additional requirements under consideration:

- Address a clear and describable risk "related to an observed or known improper or illegal" transfer of U.S. government-supported research and development (R&D) to a foreign country of concern.

- Are relevant to all fields of R&D conducted at the Covered Institution, including R&D areas that present minimal or no risk of U.S.-government supported R&D transfer to a foreign country of concern.
- Impose a substantial burden on the Covered Institution, particularly if it is a less resourced institution.
- Require the provision of supplemental funds to the Covered Institution to permit the institution to satisfy the additional requirement(s).

Applicability of the Guidelines: Unlike the draft version, the Guidelines provide specific references for institutions to use in determining whether they meet the $50 million financial threshold for the establishment of a security program. Specifically, the Guidelines provide the following definition of "Covered Institution":

> For purposes of this guidance, a participant in the U.S. R&D enterprise is a "covered institution" if and only if (A) it is an institution of higher education, a federally funded research and development center (FFRDC), or a nonprofit research institution; and (B) it receives in excess of $50 million per year, in fiscal year 2022 constant dollars, under (1) the three-year average of federal R&D obligations provided to participants in the U.S. F&D enterprise as reported in the most recent version of the Survey of Federal Science and Engineering Support to Universities, Colleges, and Nonprofit Institutions;[1] or (2) the three-year average of federal R&D obligations to FFRDCs as provided in the most recent versions of the Survey of Federal Funds for Research and Development.[2]

Additionally, federal research funding agencies are "encouraged to adopt research security requirements similar to those in this memorandum for non-covered institutions that meet the funding threshold" set forth in part (B) of the foregoing definition.

Definitions: Aside from the definitions of "Covered Institution" and "Non-covered Institution," the Guidelines do not contain new definitions for defined terms used in the document. Rather, the Guidelines refer to existing definitions for these terms that are set forth in statutes, regulations, or NSPM-33. The main definitional reference cited is the CHIPS & Science Act of 2022.

Required Elements of a Research Security Program and Certification that Covered Institution has a Security Program: Each Covered Institution's research security program must include the following four elements: (a) Cybersecurity; (b) Foreign Travel Security; (c) Research Security Training; and (d) Export Control Training, as appropriate.

[1] https://ncses.nsf.gov/surveys/federal-support-survey/2022
[2] https://ncses.nsf.gov/surveys/federal-funds-research-development/2022-2023

Institutions must certify that they have a research security program that includes these elements. The Guidelines do not describe the mechanism per which institutions will provide this certification to federal agencies. Rather, they state that within 90 days of the Guidelines' issuance, the NSTC Subcommittee on Research Security "will provide agencies with additional details on a system for U.S. government collection of certifications from covered institutions."

Specifications for Cybersecurity: IHEs are required to certify that the institution will implement a cybersecurity program that is consistent NIST's publication of the final version of NIST IR 8481: Cybersecurity for Research Findings and Possible Paths Forward (Aug. 31, 2023). IHEs will have one year after the publication of the NIST document to implement a cybersecurity program that meets the document's requirements. Non-IHEs are required to certify that they will implement a cybersecurity program that is consistent with another "relevant cybersecurity resource maintained by NIST or another federal research agency" that is not specifically named in the Guidelines.

Notably, the referenced NIST document does not identify a specific cybersecurity framework or set of practices that institutions are required to follow. Rather, it constitutes a summary of the study used to create NIST IR 8481, a description of broad categories risks and challenges that research institutions face in the cybersecurity landscape, recommendations for future work, and next steps, along with an appendix of NIST resources for managing cybersecurity risks. The "next steps" include determining "whether additional cybersecurity resources can be tailored for" for general audiences and specific fields of study, as well as coordination "with other federal agencies on cybersecurity for research contexts" and promotion of "consistent application of NIST guidance." Accordingly, it remains to be seen what will emerge as the ultimate cybersecurity resource.

Specifications for Travel Security: The Guidelines require Covered Institutions to provide periodic training on foreign travel security and implement a foreign travel reporting program as follows:

- ***Foreign Travel Security Training***: Each Covered Institution must certify that it will provide "Covered Individuals" (as defined in the CHIPS and Science Act of 2022) who are "engaged in international travel, including sponsored international travel, for organization business, teaching, conference attendance, or research purposes" with periodic training on foreign travel security. This training must initially be provided within one year after a federal research agency makes a "foreign travel security training resource" available, and thereafter, at least once every six years.

  The Guidance goes on to note that training modules provided by federal research agencies constitute such a "resource," and that NSF, NIH, Department of Energy, Department of Defense, Department of State are coordinating through the NSTC Subcommittee on Research Security to contract for the production of a foreign travel security training module. The Guidelines do not provide a timeline for the module's development.

- ***Foreign Travel Reporting Program***: In addition to foreign travel training requirements, Covered Institutions must implement a "travel reporting program" that includes an "organizational record of international travel" "for covered individuals participating in R&D awards when a federal research agency has determined that security risks warrant travel reporting in accordance with the terms of an R&D award."[3]

  As drafted, the reporting program requirement applies to persons who (a) meet the definition of "Covered Individual"; and (b) are participating in an R&D award that the federal research agency has determined presents security risks that warrant travel reporting and includes this requirement in the award terms. This approach differs from the broader language of the NSPM-33 Implementation Guidance.[4]

In terms of the types of travel that are covered under the reporting requirements, the provision makes no explicit reference to including a Covered Individual's personal travel within its scope. However, in providing examples of covered travel, the provision is unclear as to whether the listed examples are exclusive or non-exclusive. Further, the provision does not address travel that is undertaken for one purpose and then incidentally includes one of the other specified activities (e.g., personal travel to a country undertaken for vacation purposes and delivery of an impromptu lecture while visiting).

Specifications for Research Security Training: Each Covered Institution must certify that it has "implemented a research security training program for all covered individuals to address the unique needs, challenges, and risk profiles of covered individuals" and that each Covered Individual completes this training. This requirement may be met in one of two ways:

- Certification that Covered Individuals are required to complete, and have completed, the training modules that NSF has published (or successor training developed by the federal government).
- Certification that Covered Individuals are required to complete, and have completed, a research security training program that (a) includes explicit examples of behaviors that have resulted in "known improper or illegal transfer of U.S. government-supported R&D in the context of the research environment, as described to the covered institution by federal research agencies"; and (b) communicates to Covered Individuals "the importance of U.S. researcher participation in global discoveries, including attracting foreign talent to U.S. research institutions, as a core principle of maintaining international leadership and national security."

---

[3] *In implementing this requirement, institutions must also consider any separate agency requirements for reporting sponsored or reimbursed travel (e.g., NIH conflict of interest regulations at 42 C.F.R. §50.603, definition of "significant financial interest").*

[4] *NSPM-33 Implementation Guidance (Jan. 2022) at p. 18 ("Foreign travel security. Agencies should require that research organizations maintain international travel policies for faculty and staff traveling for organization business, teaching, conference attendance, research purposes, or any offers of sponsored travel that would put a person at risk. Such policies should include an organizational record of covered international travel by faculty and staff and, as appropriate, a disclosure and authorization requirement in advance of international travel, security briefings, assistance with electronic device security (smartphones, laptops, etc.), and pre-registration requirements.").*

The Guidelines specify that "a covered institution's certification requirement is met" when it provides a written or electronic attestation to a federal research funding agency that it "meets the relevant research security program requirements." As previously noted, details on the institutional certification system are forthcoming. Additionally, each Covered Individual must certify that they have completed research security training. The Guidelines do not address the mechanism for this individual certification, but as with other research security-related certifications, it may be included in proposal application forms.

Specifications for Export Control Training: Covered Institutions must certify that Covered Individuals "who perform R&D involving export-controlled technologies"[5] complete training on U.S. export control and compliance requirements. This requirement may be met in one of two ways:

- Certification that such Covered Individuals have completed "relevant trainings" administered by the Department of Commerce's Bureau of Industry and Security (BIS).[6]
- Certification that such Covered Individuals are required to complete training on complying with (a) U.S. export control and compliance requirements; and (b) requirements and processes for reviewing foreign sponsors, collaborators, and partnerships.

Notably, the Guidelines do not cite specific BIS training modules that must be included as a part of required export control training. It is unclear whether agencies are expected to provide additional specificity in their implementation plans, or whether institutions will have complete latitude in this regard.

Additional Principles that Federal Research Funding Agency are Instructed to Follow in Implementing the Guidelines: The Guidelines call for research funding agencies to follow the broad principles set forth below in implementing the Guidelines; however, the Guidelines do not provide much in the way of specific instructions or examples for their implementation:

- Prohibit discrimination, stigmatization, or targeting, on the basis of race, color, ethnicity, religion, sex (including gender, pregnancy, and sexual orientation), national origin, age (i.e., 40 or older), disability, or genetic information. Federal research agencies must require Covered Institutions to certify that they have implemented safeguards to protect the rights of researchers, students, and

[5] *The Department of Commerce Export Administration Regulations (EAR) considers technology that arises during, or that results from, fundamental research as being exempt from export control regulations. [15 C.F.R. §734.8]. The Department of State and Department of Energy maintain similar positions in their respective export control regulations. [22 C.F.R. §120.34 & 10 C.F.R. §810.2]. This exclusion is commonly referred to as the "fundamental research exemption" (FRE). However, R&D results not considered fundamental research, as well as controlled research inputs (e.g., highly controlled equipment, third-party proprietary data, technical data subject to International Traffic in Arms Regulations) would be subject to export control regulations and considered "export-controlled technologies." Universities typically manage risks associated with R&D involving export-controlled technologies via technology control plans that frequently include mandatory export controls training for individuals subject to the plans.*

[6] *Note that the Guidelines also reference publicly available resources from the Department of State, Directorate of Defense Trade Controls, and states that these resources may assist an institution "in developing its own individually tailored and robust compliance programs."*

research support staff, and the Guidelines note that many institutions must already comply with similar requirements under cited civil rights statutes.

- Provide flexibility for institutions to structure their research security programs to best serve their needs and to leverage existing programs and resources.
- Reduce administrative burden on Covered Institutions and Covered Individuals, with particular attention paid to administrative burden on less resourced institutions. In this respect, federal research funding agencies are expected to provide institutions with technical assistance and other resources to aid in compliance.
- Minimize impact to smaller institutions to facilitate their participation in federal R&D programs.

COGR will continue to evaluate these Guidelines and consult with COGR members on areas of the Guidelines that require further elaboration or clarification. If you have any questions about this document, please contact memberservices@cogr.edu.

COGR is an association of over 200 public and private U.S. research universities and affiliated academic medical centers and research institutes. We focus on the impact of federal regulations, policies, and practices on the performance of research conducted at our member institutions, and we advocate for sound, efficient, and effective regulation that safeguards research and minimizes administrative and cost burdens. For more information on COGR, visit www.cogr.edu.