



# Safeguarding Science

An Outreach Initiative for  
Protecting Research and  
Innovation in Emerging  
Technologies

An informed, empowered scientific community is best positioned to assess emerging technologies and their applications and to design measures to guard against their potential misuse or theft. The National Counterintelligence and Security Center (NCSC) has partnered with multiple federal agencies to develop an outreach initiative, “Safeguarding Science,” designed to raise awareness of the spectrum of risk in emerging technologies and to help stakeholders in these fields to develop and utilize methods to protect research and innovation.

As mandated by Congress, a core NCSC mission is to conduct counterintelligence (CI) outreach to the U.S. private sector, academic and research communities, as well as other external stakeholders to arm them with information about foreign intelligence threats to their organizations and ways to mitigate risk.

## Safeguarding Science Toolkit

The resources below have been developed with the following partners and other federal agencies.

- [National Science Foundation](#)
- [National Institute of Standards and Technology](#)
- [U.S. Department of Health and Human Services](#)
- [Federal Aviation Association](#)
- [U.S. Department of War](#)

The toolkit provides partners with a range of resources to choose from to help them better protect their research and innovation. The resources include training, best practices, videos, awareness materials, policy references, and other materials from across the U.S. government, as well as from academia (including training for research institutions made by research institutions). The toolkit will remain a dynamic resource that is maintained and updated. Select a category to start accessing resources.





## Safeguarding Science Goals

- Promote a U.S. research ecosystem that emphasizes collaboration, openness, equity, integrity, and security, all of which facilitate innovation
- Provide curated resources for our stakeholders to support best practices in protecting research and innovation
- Assist academia and industry in developing their own methods to protect research from theft, misuse, abuse, or exploitation.
- Foster information exchanges to better identify emerging technology security challenges

## Research Security

The National Science Foundation's (NSF) Office of the Chief of Research Security Strategy and Policy (OCRSSP) hosts many resources regarding best practices in research security for the academic community on their research security website. The [NSF Research Security website](#) includes updates on research security activities being conducted by the Office of the CRSSP, summaries of issues relevant to foreign interference and risk mitigation, and additional resources for reference.

NSF also provides guidance and references related national Security Presidential Memorandum on United States Government-Supported Research and Development National Security Policy 33 (NSPM-33) and [Implementation Guidance](#).

Additional guidance on research security may be found here:

- COGR is the national authority on federal policies and regulations affecting U.S. research institutions, also maintains a [Matrix of Science & Security Laws, Regulations, and Policies](#) that is updated regularly.
- The National Institutes of Health (NIH) - [Requirements for Disclosure of other Support, Foreign Components, and Conflicts of Interest](#) provides information on applicant and recipient institution responsibilities, a chart on disclosure requirements, and details NIH's responsibilities in the grant award process.
- The Department of Energy (DOE) - PF 2022-32 Department of Energy Current and Pending Support Disclosure Requirements for Financial Assistance (Jun 2022) provided information and guidance regarding DOE's implementation of NSPM-33 on National Security Strategy for United States Government-Supported Research and Development, issued January 2022. More information relevant to disclosure requirements and standardization, see the [Financial Assistance Letter](#).

Links to any non-Governmental information are provided for reference and awareness, and not as directions or NCSC recommendations.

The initiative focuses on emerging technology sectors where the stakes are potentially greatest for U.S. economic and national security.





## Additional Resources

The National Counterintelligence and Security Center (NCSC) developed Supply Chain Risk Management (SCRM) resources that provide multiple resources for developing a more advanced supply chain center security plan. This toolkit is best suited for facility security personnel, senior leaders, and employees in acquisitions-type roles. NCSC also shares threat information and counterintelligence resources for industry and academia that provide brief overviews of specific foreign intelligence threats as well as impacts of those threats and steps for mitigation, and raises awareness about supply chain threats while providing resources to mitigate risks. The [Cybersecurity & Infrastructure Security Agency](#) provides **cybersecurity resources** that are relevant to safeguarding science and research security.

The [Association of American Universities](#) provides **academic resources** specific to research institutions regarding safeguarding science and research security.

The [Defense Counterintelligence and Security Agency Center for Development of Security Excellence](#) provides relevant **insider threat program and unauthorized disclosure resources** designed to deter, detect, and mitigate actions by insiders who represent a threat to national security.

