Science and Security Landscape

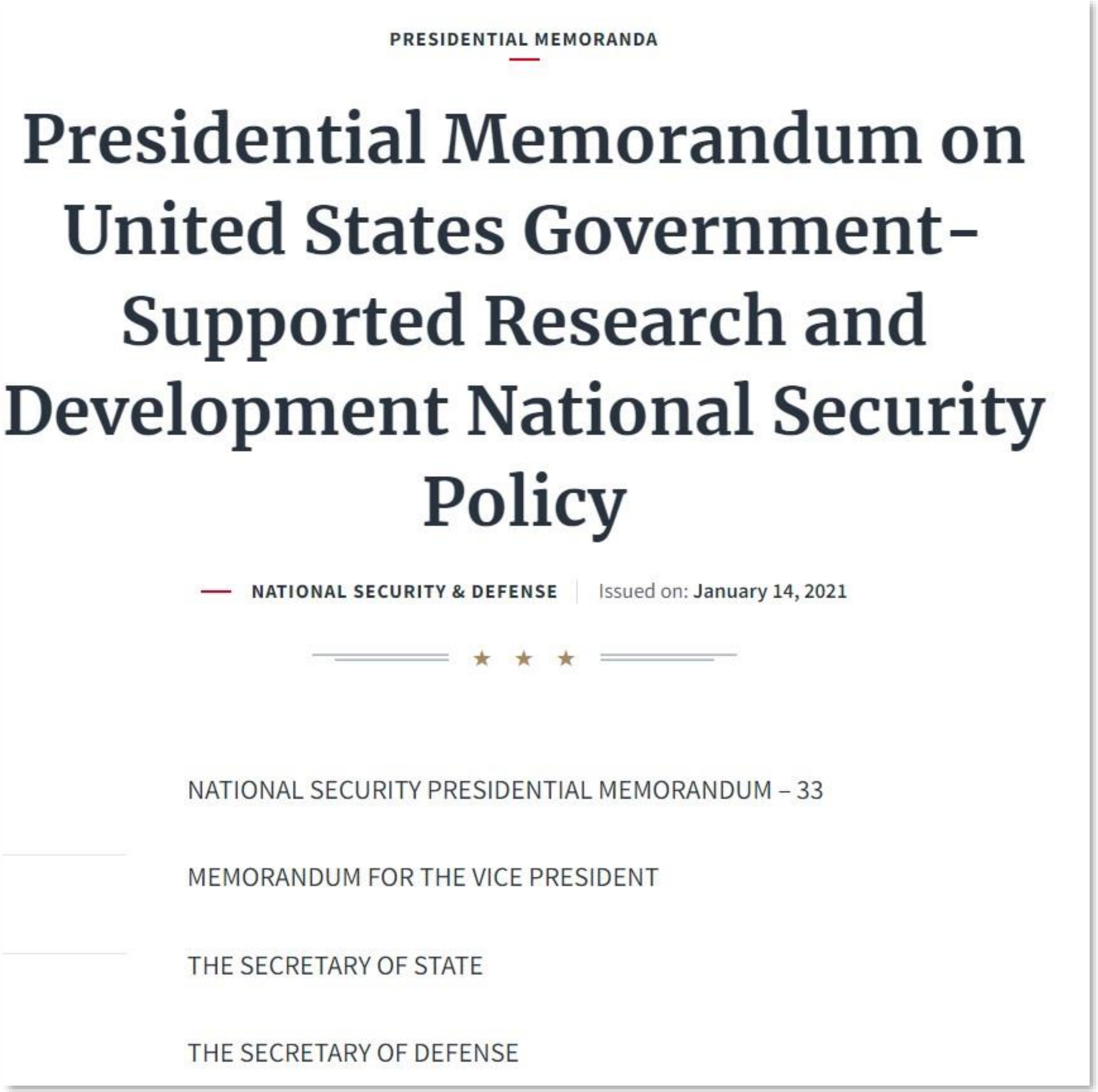
Legislation:

- **Sec. 1746, FY 2020 National Defense Authorization Act**: Directs OSTP to create an interagency working group “to protect federally funded research and development from foreign interference” and establishes a National Academies Roundtable
- **Sec. 223, FY 2021 National Defense Authorization Act**: Establishes funding disclosure requirements, standardization, and details consequences

Government Reports:

- NSF-commissioned report on research security by the independent JASON group
- Senate Homeland Security and Governmental Affairs Permanent Subcommittee on Investigations: hearing and report on Threats to the U.S. Research Enterprise from China’s Talent Recruitment Plans
- GAO report: Agencies Need to Enhance Policies to Address Foreign Influence

NSPM-33 and Recommendations



PRESIDENTIAL MEMORANDA

Presidential Memorandum on United States Government-Supported Research and Development National Security Policy

NATIONAL SECURITY & DEFENSE | Issued on: January 14, 2021

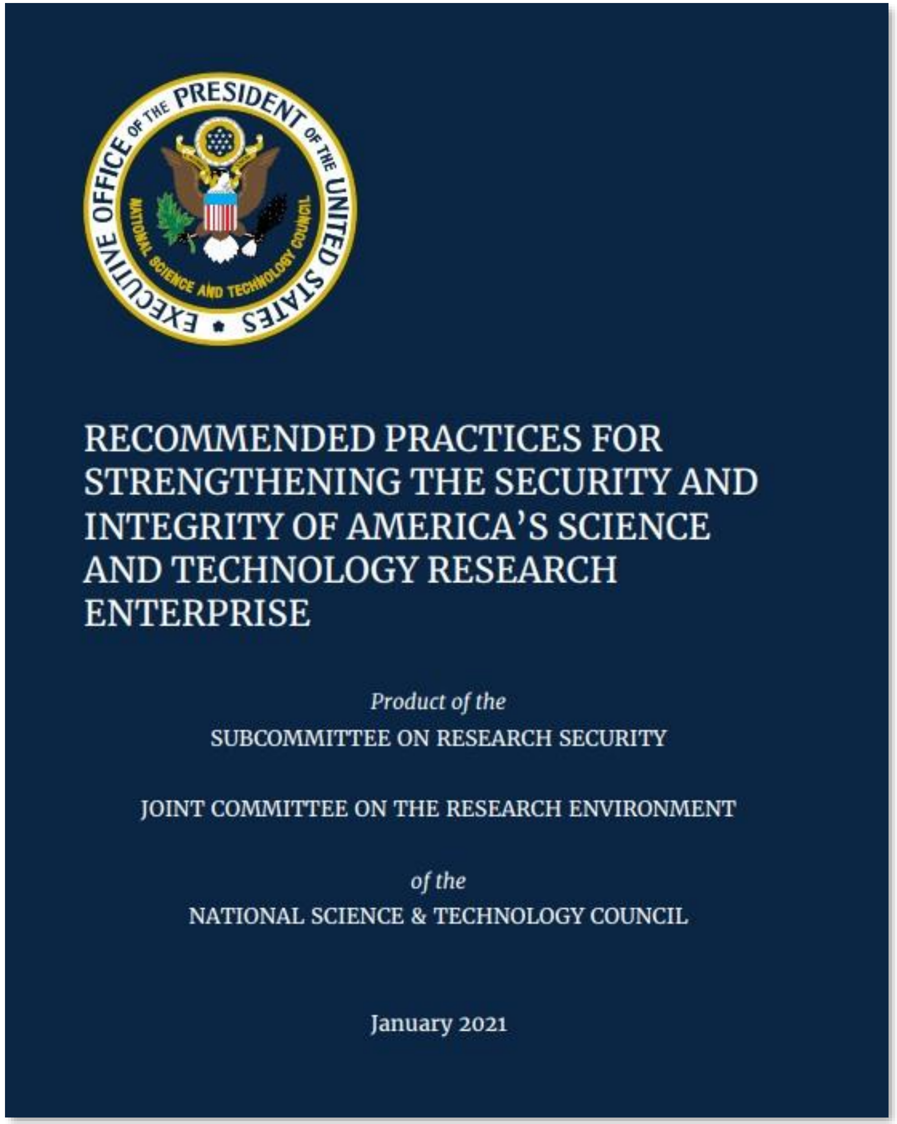
★ ★ ★

NATIONAL SECURITY PRESIDENTIAL MEMORANDUM – 33

MEMORANDUM FOR THE VICE PRESIDENT

THE SECRETARY OF STATE

THE SECRETARY OF DEFENSE



EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES
NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

RECOMMENDED PRACTICES FOR STRENGTHENING THE SECURITY AND INTEGRITY OF AMERICA'S SCIENCE AND TECHNOLOGY RESEARCH ENTERPRISE

Product of the

SUBCOMMITTEE ON RESEARCH SECURITY

JOINT COMMITTEE ON THE RESEARCH ENVIRONMENT

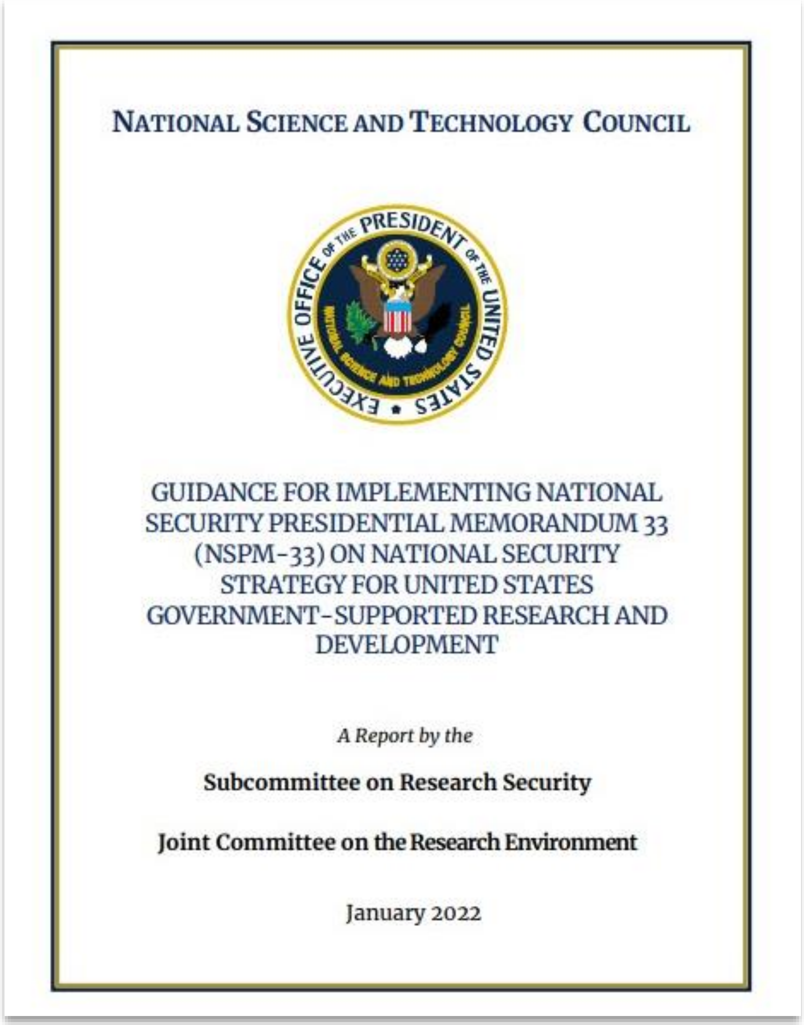
of the

NATIONAL SCIENCE & TECHNOLOGY COUNCIL

January 2021

NSPM-33 Implementation Guidance

- **Reaffirm core values:** openness, transparency, honesty, equity, fair competition, objectivity, and democratic values
- **Acknowledge the seriousness of the challenge:** some foreign governments are attempting to acquire our most advanced knowledge and technologies
- **Communicate and apply policies in a clear and uniform way:** policies must not fuel xenophobia or other forms of discrimination
- **Continue welcoming international students, scholars, and collaborations:** this openness is among the country's greatest strengths



NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

GUIDANCE FOR IMPLEMENTING NATIONAL SECURITY PRESIDENTIAL MEMORANDUM 33 (NSPM-33) ON NATIONAL SECURITY STRATEGY FOR UNITED STATES GOVERNMENT-SUPPORTED RESEARCH AND DEVELOPMENT

A Report by the

Subcommittee on Research Security

Joint Committee on the Research Environment

January 2022

NSPM-33: Key Provisions

1. **Disclosure Requirements and Standardization**
2. **Digital Persistent Identifiers**
3. **Consequences for Violating Disclosure Requirements**
4. **Agency Information Sharing**
5. **Research Security Programs**

NSPM-33 Key Provisions: Disclosure Requirements and Standardization

- With respect to research security, ensure federally funded researchers and research organizations provide the appropriate information regarding:
  - Potential conflicts of interest
  - Potential conflicts of commitment
- Advance standardization in disclosure requirements across agencies

NSPM-33 Key Provisions: Digital Persistent Identifiers

- Encourage the use of digital persistent identifiers (DPIs), e.g., electronic CVs, in disclosure processes to bolster security while reducing burden

- Encourage creators of DPI services to include categories of information that can identify and avoid financial conflicts of interest and conflicts of commitment

NSPM-33 Key Provisions: Consequences for Violating Disclosure Requirements

- Consequences can include criminal, civil, and/or administrative actions
- The Guidance encourages and ensures mechanisms for researchers to correct existing disclosures
- A variety of factors should be considered when considering consequences:
    - Harm or potential harm to the Federal Government, U.S. taxpayers, and other National interests;
    - Intent;
    - Knowledge of requirements;
    - Pattern of violation vs. isolated incident;
    - Existence and timing of self-disclosure;
    - Policies, practices, and training available

NSPM-33 Key Provisions: Information Sharing within the Federal Government

- The Guidance directs research agencies to share information about violations of disclosure requirements

- Must be consistent with due process, privacy considerations, and all other applicable laws

- Information sharing will take place through a centralized government portal, SAM.gov

NSPM-33 Key Provisions: Research Security Programs

- NSPM-33 requires a certification from research organizations awarded $50M or more in federal awards that research security programs have been implemented

- Research security programs should include:
  - Cybersecurity
  - Foreign travel security
  - Research security training
  - Export control training, as appropriate

- The federal government will provide standardized technical assistance to develop the content of the programs

Next Steps

- Development of standardized **formats** and accompanying instructions for disclosures in **award proposals over the next 120 days (by June 2022)**
- Clarification on DPI usage
- Standardization of **research security program requirements** and certifications
- Coordination on communicating to researchers and research organizations **how agencies use disclosure information** in making decisions about research funding and support
- **Assessment** of agency implementation and iterative **improvement** of research security policies