

Research Security: A Global Challenge with Local to Global Implications

Kelvin K. Droegemeier
Department of Atmospheric Sciences
University of Illinois Urbana-Champaign

NASEM Meeting of Experts: Assessing Research Security Efforts in Higher Education
16 September 2024

THE WHITE HOUSE
WASHINGTON
January 14, 2021

NATIONAL SECURITY PRESIDENTIAL MEMORANDUM - 33

MEMORANDUM FOR THE VICE PRESIDENT
THE SECRETARY OF STATE
THE SECRETARY OF DEFENSE
THE ATTORNEY GENERAL
THE SECRETARY OF THE INTERIOR
THE SECRETARY OF AGRICULTURE
THE SECRETARY OF COMMERCE
THE SECRETARY OF HEALTH AND HUMAN SERVICES
THE SECRETARY OF TRANSPORTATION
THE SECRETARY OF ENERGY
THE SECRETARY OF EDUCATION
THE SECRETARY OF VETERANS AFFAIRS
THE SECRETARY OF HOMELAND SECURITY
THE ASSISTANT TO THE PRESIDENT
THE ADMINISTRATOR OF THE ENVIRONMENTAL PROTECTION AGENCY
THE DIRECTOR OF THE OFFICE OF MANAGEMENT AND BUDGET
THE DIRECTOR OF NATIONAL INTELLIGENCE
THE DIRECTOR OF THE CENTRAL INTELLIGENCE AGENCY
THE ASSISTANT TO THE PRESIDENT FOR NATIONAL SECURITY AFFAIRS
COUNSEL TO THE PRESIDENT
ASSISTANT TO THE PRESIDENT, DEPUTY ASSISTANT TO THE PRESIDENT FOR NATIONAL SECURITY
NATIONAL SECURITY COUNCIL LEGAL ATTACHÉ
THE DIRECTOR OF THE OFFICE OF SCIENCE AND TECHNOLOGY POLICY
THE DIRECTOR OF THE NATIONAL SCIENCE AND TECHNOLOGY COUNCIL
THE ADMINISTRATOR OF THE NATIONAL SPACE ADMINISTRATION
THE DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION
THE SECRETARY OF THE SMITHSONIAN INSTITUTION
THE DIRECTOR OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

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

136 STAT. 1366

PUBLIC LAW 117-167—AUG. 9, 2022

Public Law 117-167 117th Congress

An Act

Making appropriations for Legislative Branch for the fiscal year ending September 30, 2022, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. TABLE OF CONTENTS.

The table of contents for this Act is as follows:

- Sec. 1. Table of contents.
Sec. 2. References.

DIVISION A—CHIPS ACT

- Sec. 101. Short title.
Sec. 102. Creating helpful incentives to promote semiconductor research and development.
Sec. 103. Semiconductor incentives.
Sec. 104. Opportunity and inclusion.
Sec. 105. Additional GAO reporting requirements.
Sec. 106. Appropriations for wireless supply chain.
Sec. 107. Advanced manufacturing investments.

DIVISION B—RESEARCH SECURITY

- Sec. 10000. Table of contents.
Sec. 10001. Short title.
Sec. 10002. Definitions.
Sec. 10003. Budgetary effects.

TITLE I—DEPARTMENT OF ENERGY

- Sec. 10101. Mission of the Office of Science.
Sec. 10102. Basic energy sciences program.
Sec. 10103. Biological and environmental research.
Sec. 10104. Advanced scientific computing research.
Sec. 10105. Fusion energy research.
Sec. 10106. High energy physics program.
Sec. 10107. Nuclear physics program.
Sec. 10108. Science laboratories infrastructure.
Sec. 10109. Accelerator research and development.
Sec. 10110. Isotope research, development, and production.
Sec. 10111. Increased collaboration with the private sector.
Sec. 10112. High intensity laser research and development.
Sec. 10113. Established program to stimulate research and development.
Sec. 10114. Research security.

TITLE II—NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

- Sec. 10201. Definitions.

Subtitle A—Authorization of Appropriations

- Sec. 10211. Authorization of appropriations.



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF SCIENCE AND TECHNOLOGY POLICY
WASHINGTON, D.C. 20502

July 9, 2024

MEMORANDUM FOR THE HEADS OF FEDERAL RESEARCH AGENCIES

FROM: Arati Prabhakar
Assistant to the President for Science and Technology
Director of the Office of Science and Technology Policy

SUBJECT: Guidelines for Research Security Programs at Covered Institutions

To address risks posed by strategic competitors to the U.S. research and development (R&D) enterprise, the Biden-Harris Administration is implementing several measures to improve research security while preserving the openness that has long enabled U.S. R&D leadership throughout the world and without exacerbating xenophobia, prejudice, or discrimination.

This memorandum provides federal research agencies with guidelines for implementing a certification requirement imposed by National Security Presidential Memorandum-33 (NSPM-33).¹ Specifically, federal research agencies must require certain research institutions (“covered institutions”) to certify to the funding agency that the institution has established and operates a research security program, including several specific elements described in detail below.

These guidelines are issued in accordance with NSPM-33 and certain provisions of Public Law 117-167 (the CHIPS and Science Act).² The White House Office of Science and Technology Policy (OSTP)—in consultation with National Science and Technology Council (NSTC) Subcommittee on Research Security, the Office of Management and Budget (OMB), and stakeholders—is responsible for developing a “standardized requirement” for “uniform implementation” across federal research agencies.³ This memorandum describes and sets forth that standardized requirement.⁴ It reflects the significant work of the NSTC Subcommittee on

¹ “Presidential Memorandum on United States Government-Supported Research and Development National Security Policy.” The White House (January 14, 2021) §4(g). <https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/>

² Pub. L. 117-167 §10634, 42 U.S.C. §19234. <https://www.congress.gov/bills/117/congress-house-bill/4346/text>

³ “Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development.” National Science and Technology Council (NSTC), January 2022, pp.18-21. <https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf>

⁴ This guidance is intended to be consistent with NSPM-33 and relevant portions of the CHIPS and Science Act. It supersedes, in full, the portions of the NSTC Implementation Guidance describing Research Security Programs (see, in particular, pp. 18-21). With respect to section 4(g) of NSPM-33, the guidance in this memorandum sets forth the “standardized requirement” for “uniform implementation” across federal agencies, as contemplated by the NSTC

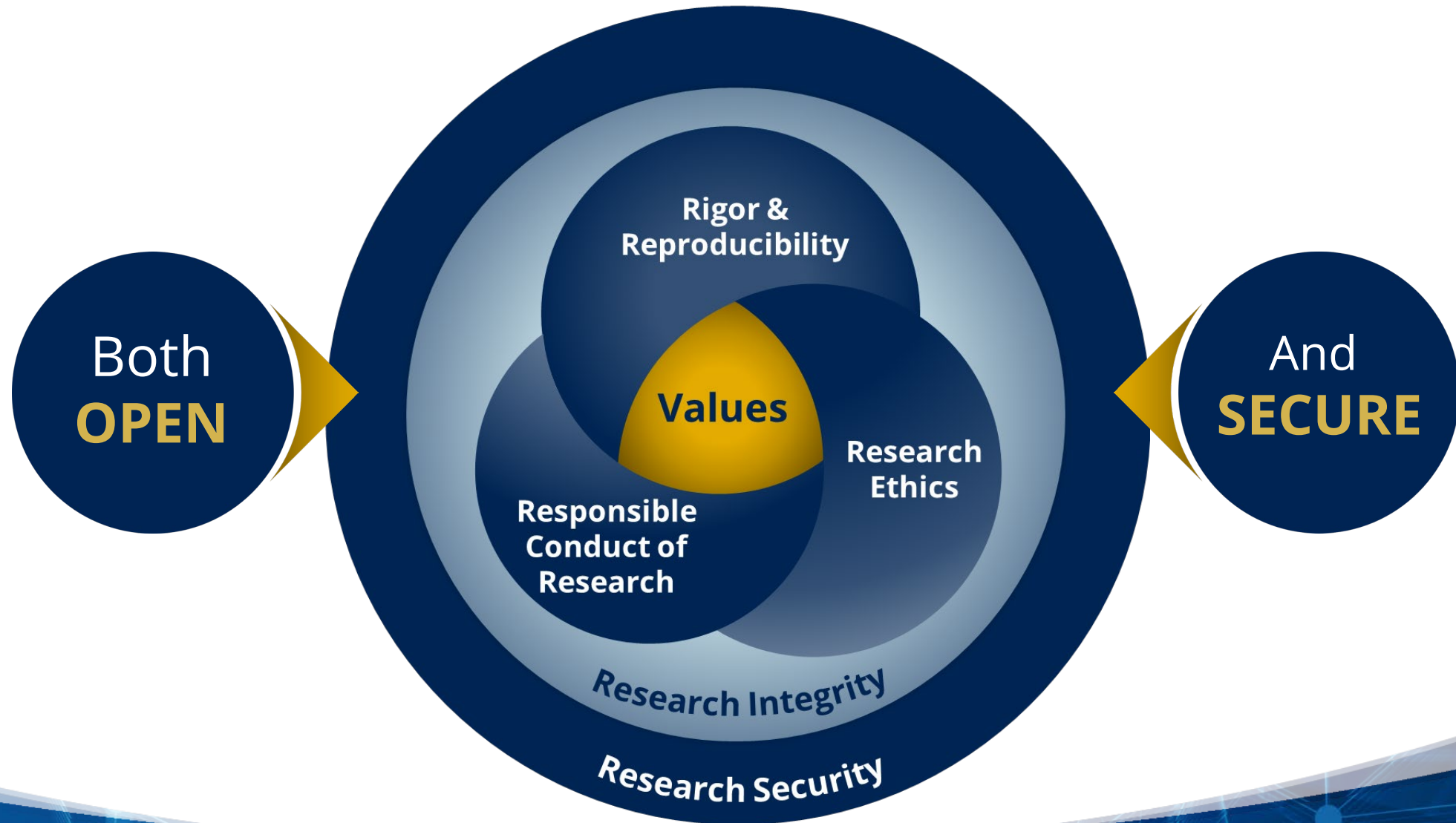
Lots of Agency Actions

- NSF: SECURE Center, TRUST Program, Research on Research Security (RoRS) Program
- NIH: Decision Matrix
- DOE: Risk Matrix, several Orders and Policies
- DOD: Decision Matrix
- NIST: Framework in Internal Reports 8481, 8484,
- Others...

$$\text{U.S. Global Competitiveness} \propto \frac{\text{Capabilities and Investments}}{\text{Threats/Interference **to our VALUES**}}$$

Because values underpin the research process itself, threats to our values translate into threats to research and thus to our national and economic security

Values are the Heartbeat of Research Security



Research Security

- “**Safeguarding** the research enterprise against the **misappropriation** of research and development to the **detriment** of national or economic security, related violations of research **integrity** and foreign government **interference**.” (NSPM-33 Implementation Guidance)

Research Integrity

- “The use of **honest and verifiable** methods in proposing, performing and evaluating research; reporting research results with particular attention to adherence to **rules, regulations and guidelines**; and following commonly accepted professional **codes or norms**.” (NSPM-33 Implementation Guidance)

What are We Trying to Achieve or Maintain?

- **Global leadership** in science and technology research & education
- **Freedom** to explore, create, develop, deploy and benefit from research
- Ability to freely and globally **collaborate** in principled ways
- **Protection** of our assets against malign actors
- Uniform application of **values** and ethical principles
- **Ethical and trustworthy** use of research outcomes
- An appropriately structured **regulatory environment**
- → Promotion and modeling of **democracy** for the world

And of Course, the Ever-Present Challenge



UNIVERSITY OF
ILLINOIS
URBANA-CHAMPAIGN

Different Stakeholders, Different Lenses

- Seriousness and prevalence of the **challenges/threats**
- Appropriateness of **actions** being taken
- Points of **responsibility**
- **Resources** available
- **Implications** and intended & unintended consequences
- Definitions and measures of **impact** and **success**



Different Stakeholders, Different Lenses

Other Nations
The President and EOP
Congress
Cabinet Secretaries and Equivalent
Agency Heads and Senior Staff
Chancellors, Presidents, Boards
Company Leaders and Boards
Vice Chancellors for Research
Agency Program Officers
Sponsored Programs Staff
Individual Researchers

The Public – Funding Research and Benefitting from it



UNIVERSITY OF
ILLINOIS
URBANA-CHAMPAIGN

Q1: How Should we Think About Effectiveness?

- As a highly **individual** to **multinational** concept
- As having both **quantitative** (e.g., number of reductions in misappropriation) and **qualitative** (e.g., culture change) dimensions
- As having both **direct** and **indirect** effects
- As requiring **baseline data** (both quantitative and qualitative) against which progress can be measured
- As requiring **different approaches** of measurement and communication for different categories of stakeholders
- As needing to consider both **outcomes** (actions taken) and their **impacts**

Q1: Some Important Items to Assess

- Researcher **understanding** of research security as it relates to them personally, the US research enterprise, and the global enterprise
- Researcher ability to **identify** problematic situations
- **Additional** compliance regulations put forth by institutions
- Availability and use of **tools** for making security-informed decisions
- Institutional **culture** and **leadership** awareness/support
- Administrative **workload** associated with research security compliance (researchers, institutions, agency staff)
- Number of research security **“incidents”**

Q2: How Should we Think About Impacts of Research Security Policies and Requirements?

- As having highly **individual** to **global** implications
- As having a broad range of **timescales** over which to manifest and remain
- As having both **positive** (e.g., reducing foreign government interference) and **negative** (e.g., administrative workload, perceptions) dimensions
- As having **expected and unintended** consequences
- As needing to be **messaged** differently across stakeholder groups
- As being somewhat in the **eye of the beholder**, politically and socially, despite authoritative measurement results

Q2: Some Positive Impacts

- **Protecting researcher** ideas, intellectual property, integrity and reputation
- Helping keep **America at the forefront** of S&T and preventing our adversaries from benefitting at our expense
- Promoting our (and research) **values** in a very visible, tangible and continuous manner
- Helping researchers who were educated and trained in a **different value system** see the importance of our values, and how adhering to them positively impacts research and those who benefit from its outcomes
- Demonstrating the value of **democracy** to those who oppose it

Q2: Some Negative Impacts

- Playing into the hands of our **adversaries** by adding administrative activities that otherwise would be unnecessary, thus wasting intellectual horsepower
- Additional **administrative workload** for researchers, their institutions, and funding organizations
- Chilling impact on **international collaboration**
- A sense by some of **ethnic profiling** and **xenophobia**
- Failure to **reduce** administrative workload of other compliance rules and regulations that are no longer effective

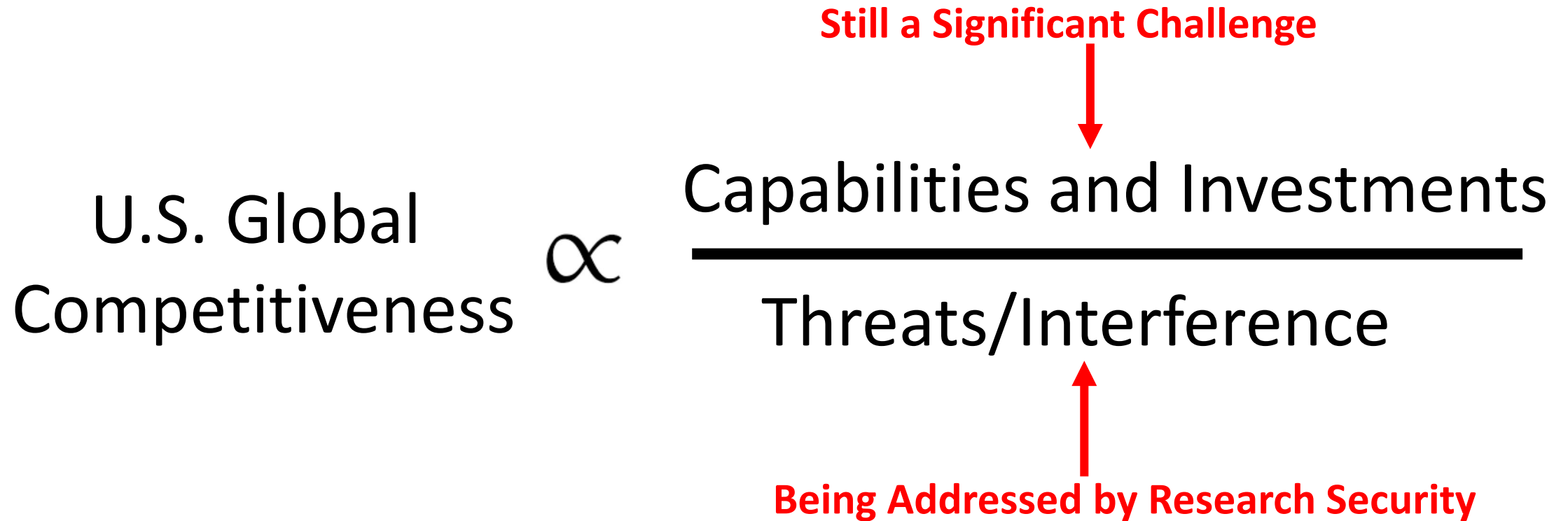
Q3: Where are the Holes?

- Having a much clearer picture of the following **threat attributes**: forms, frequency of occurrence, levels of risk (real and perceived), changing characteristics over time, role of intermediary actors, and risks to smaller institutions. The NSF **Research on Research Security Program** will help.
- **Differences of risk** across disciplines and individual projects
- Ability to know when fundamental research evolves into a state where it requires **special** research security considerations (e.g., dual-use)
- A formal effort to reduce administrative workload in **other areas** as research security compliance requirements grow

$$\text{U.S. Global Competitiveness} \propto \frac{\text{Capabilities and Investments}}{\text{Threats/Interference}}$$

Still a Significant Challenge

Being Addressed by Research Security



Final Thoughts

- The United States should **not play to not lose**: a strong **offense** is critical
- Global **platforms** present new challenges (AI, 5G, CRISPR, etc)
- However! Those who **develop** tools usually are the best at **using** them and creating new ones – and the US is **THE world leader** in innovation
- The US needs to **lead from a position of strength and capability (via investment and untying our hands)** and not be a slave to ploys which cause us to divert too much attention to protection