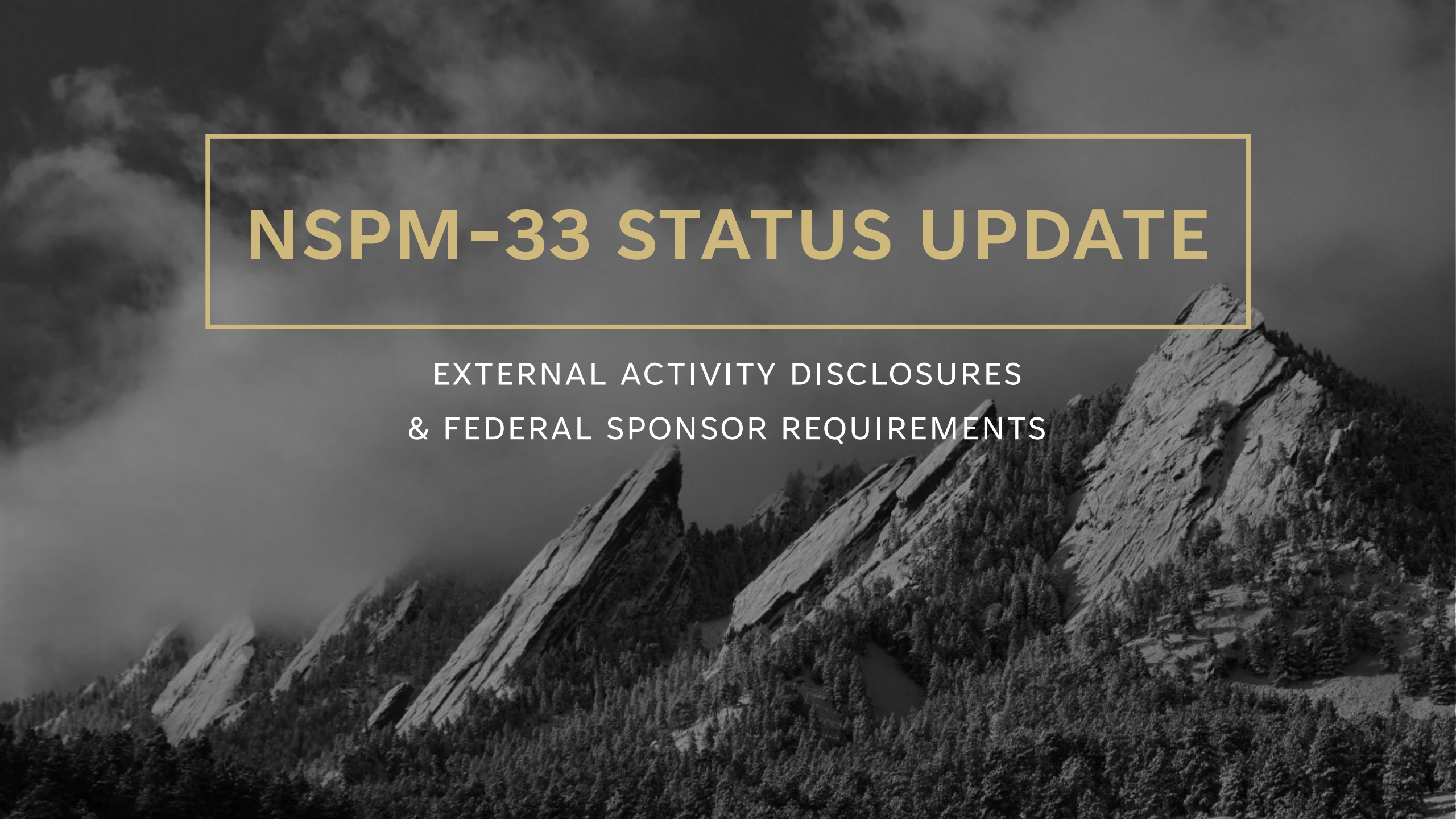


NSPM-33 STATUS UPDATE

EXTERNAL ACTIVITY DISCLOSURES

& FEDERAL SPONSOR REQUIREMENTS

PRESENTER INTRO

NIKI SPAETH

Training Manager &
Research Security
Administrator

OFFICE OF CONTRACTS & GRANTS (OCG)

nicole.spaeth@colorado.edu

OCG TRAINING PROGRAM

Oversight of the development, design and facilitation of the Office of Contracts and Grants Training Program.

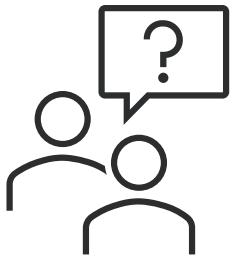
RESEARCH SECURITY

Process and manage security clearances for identified research personnel & assist in maintaining CU Boulder's National Security Program.

REVIEWING DEPA FORMS

Review DEPA forms submitted by key project personnel to ensure compliance with sponsor disclosure requirements.

PRESENTATION OVERVIEW



WHAT IS NSPM-33?

What does it require, how will it be implemented & what's the timeline?

HOW DOES IT APPLY TO CU BOULDER?

How does NSPM-33 affect our current processes around external activity disclosures?

ANTICIPATING CHANGE

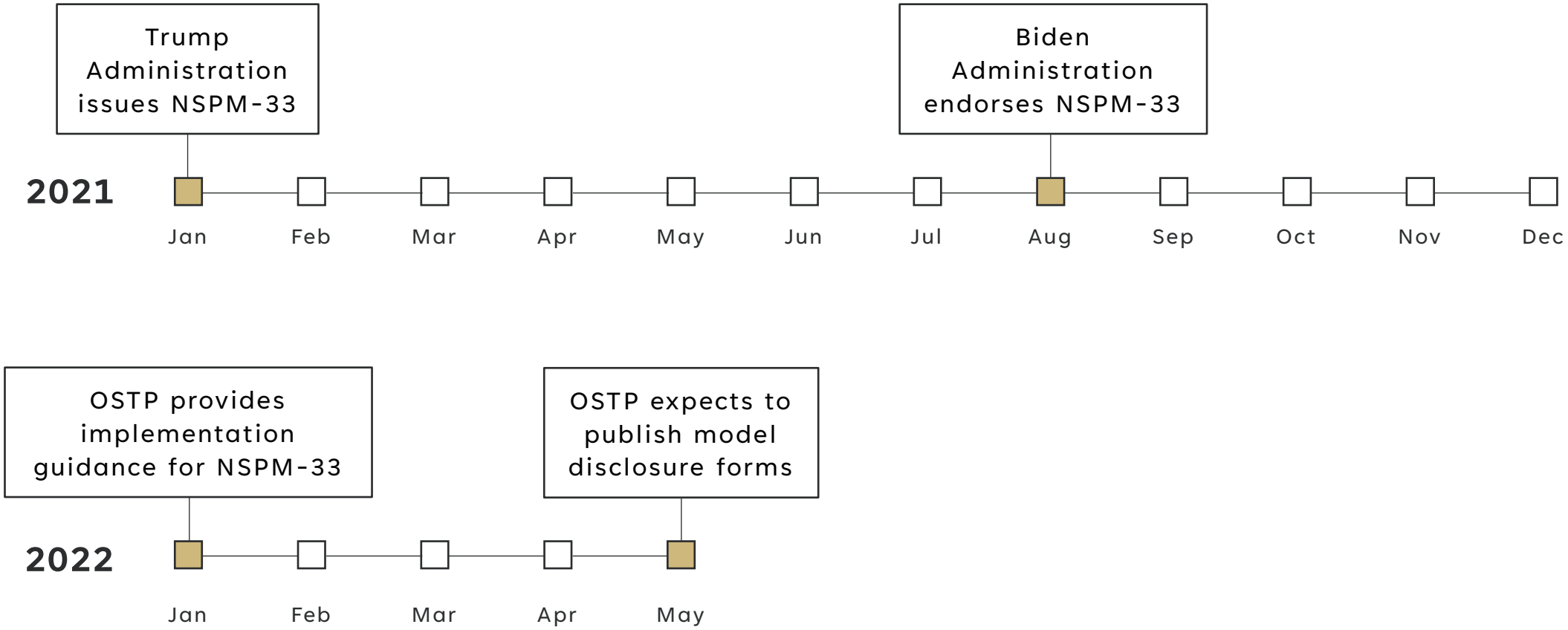
What should we expect from federal sponsors as they implement NSPM-33?

WHAT IS NATIONAL SECURITY PRESIDENTIAL MEMORANDUM 33?

WHAT IS NSPM-33? NSPM-33 is a directive from the President requiring all federal research funding agencies to strengthen and standardize disclosure requirements for federally funded awards. In addition, it also mandates the establishment of research security programs at major institutions receiving federal funds.

WHY IS IT NEEDED? There has been an increasing need to protect U.S-funded scientific research from foreign interference and exploitation, including espionage and intellectual property theft.

TIMELINE OF NSPM-33



WHAT ARE THE GOALS OF NSPM-33?

PROTECTION

To protect America's national security while promoting openness in the research community

CLARITY

To make it clear so that well-intentioned researchers can easily and properly comply

CONSISTENCY

To ensure that policies do not fuel xenophobia or prejudice

"The goal is for the government to clearly describe what it needs to know and for researchers to be able to report the same information in the same way to the greatest extent possible, regardless of which funding agency they're applying to."

-Eric Lander, former OSTP Director

IMPLEMENTATION GUIDANCE OF NSPM-33

DISCLOSURE POLICY

OVERSIGHT & ENFORCEMENT

RESEARCH SECURITY PROGRAMS

NSPM-33 DISCLOSURE POLICY

DISCLOSURE REQUIREMENTS, dictating **who** is required to disclose and what **activities** must be disclosed, will be standardized across research agencies to the greatest extent practicable.

DISCLOSURE FORMS AND FORMATS will be standardized across research agencies to the greatest extent practicable.

The use of **DIGITAL PERSISTENT IDENTIFIERS** will be encouraged to track disclosures and reduce administrative burden.

Institutions will be required to **UPDATE ALL DISCLOSURES** before an award of support, at least annually, and more frequently as agencies deem appropriate.

Research agencies will ensure that **MECHANISMS FOR CORRECTING DISCLOSURES** exist, are communicated clearly, and are simple and straightforward.

HOW THIS APPLIES TO CU BOULDER

PROPOSAL PREPARATION & AWARD MANAGEMENT

At proposal stage, OCG Proposal Analysts will partner with PIs to ensure compliance with any new disclosure requirements, forms and formats that emerge from the implementation of NSPM-33.

During the period of performance, if corrections or updates to disclosures need to be made, your department's OCG Post Award team can assist and provide guidance in accordance with NSPM-33.

USE OF ORCID (DIGITAL PERSISTENT IDENTIFIER)

Many CU Researchers use ORCID IDs, and NIH already requires PIs to be registered with ORCID. In light of NSPM-33, OCG encourages all researchers who receive or intend to apply for federal funding to register with ORCID.

OCG DEPA REVIEWS

OCG reviews submitted DEPA forms from individuals who receive federal funding and have external activities to report. In this review, OCG ensures the individual is complying with sponsor disclosure requirements for their current federal awards.

NSPM-33 OVERSIGHT & ENFORCEMENT

The failure to make or update disclosures may trigger a range of penalties, including:

CRIMINAL LIABILITY for individual researchers

CIVIL LIABILITY for research institutions under the False Claims Act

RESEARCH IMPEDIMENTS, such as terminated or suspended grants, mandatory return of research funds, or exclusion of certain personnel from research activities

TIPS TO AVOID PENALTIES

FIX ERRORS, especially before they become the subject of an inquiry. Identifying errors will not necessarily lead to investigations or enforcement actions.

DISCLOSE CONSISTENTLY ACROSS AGENCIES: Interagency sharing of information about violations of disclosure requirements, such as when administrative or enforcement action has been taken and in support of risk analysis, is encouraged.

NSPM-33 RESEARCH SECURITY PROGRAMS

NSPM-33 requires a certification from research organizations awarded in excess of $50 million per year in total Federal research funding that they have implemented a research security program that includes the **four elements** highlighted in NSPM-33:

- **CYBERSECURITY**
- **FOREIGN TRAVEL SECURITY**
- **RESEARCH SECURITY TRAINING**
- **EXPORT CONTROL TRAINING**

HOW THIS APPLIES TO CU BOULDER

OFFICE OF EXPORT CONTROLS (OEC)

Provides support and resources to assist faculty and staff with Export Control compliance. OEC can also assist with export and sanction determinations related to international travel.

CU BOULDER'S RESEARCH CYBERSECURITY PROGRAM (ITSO)

Provides support and resources to assist faculty and staff in accomplishing research activities while remaining in compliance with CUI policies and practices. The program will include CUI (Controlled Unclassified Information) and research cyber security training, consulting services, and CUI-compliant information technology (IT) services.

OCG'S NATIONAL SECURITY TEAM & RESEARCH SECURITY (RIO)

OCG has a team dedicated to assisting faculty and staff with administrative compliance required with classified government work. Furthermore, RIO is monitoring the impact of NSPM-33 and will continue to provide additional training as further information is released by the Federal Government and our sponsoring Agencies.

ANTICIPATING CHANGE

“The task ahead is to realize this vision.”

For Federal agencies, the work will include developing, **within the next 120 days**, model award proposal disclosure forms and instructions to make clear what is expected of researchers.

For qualifying research organizations (CU Boulder), a research security program should be established as soon as possible, but they will have **one year** (from date of issuance of the formal requirement) to comply.

RESOURCES

1/04/22 – NSPM-33 IMPLEMENTATION GUIDANCE

8/10/21 – BIDEN ADMIN ENDORSEMENT OF NSPM-33

1/14/21 – INITIAL ISSUE OF NSPM-33

JSPURA ARTICLE – SUMMARY OF NSPM-33

NYT ARTICLE – CONVICTION OF DR. LIEBER

CU BOULDER RESEARCH CYBERSECURITY PROGRAM

OFFICE OF EXPORT CONTROLS TRAINING

OFFICE OF EXPORT CONTROLS – INTERNATIONAL TRAVEL

OCG DIRECTORY FOR DEPARTMENTS

ORCID REGISTRATION INSTRUCTIONS

ORCID WEBSITE

SCIENCV INSTRUCTIONS